
L-INX™ Automation Server

User Manual

LOYTEC electronics GmbH



Contact

LOYTEC electronics GmbH
Blumengasse 35
1170 Vienna
AUSTRIA/EUROPE
support@loytec.com
<http://www.loytec.com>

Version 3.5

Document № 88073007

LOYTEC MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS,
EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU,
AND

LOYTEC SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF
MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THIS
PRODUCT IS NOT DESIGNED OR INTENDED FOR USE IN EQUIPMENT
INTENDED FOR SURGICAL IMPLANT INTO THE BODY OR OTHER
APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN
FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN
AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH IN THE FAILURE
OF SUCH PRODUCT COULD CREATE A SITUATION IN WHICH PERSONAL
INJURY OR DEATH MAY OCCUR.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted,
in
any form or by any means, electronic, mechanical, photocopying, recording, or otherwise,
without the prior written permission of LOYTEC.

LC3020™, L-Chip™, L-Core™, L-DALI™, L-GATE™, L-INX™, L-IP™, LPA™,
L-Proxy™, L-Switch™, L-Term™, L-VIS™, L-WEB™, and ORION™ stack are
trademarks of LOYTEC electronics GmbH.

LonTalk®, LONWORKS®, Neuron®, LONMARK®, LonMaker®, i.LON®, and LNS® are
trademarks of Echelon Corporation registered in the United States and other countries.

Contents

1	Introduction	13
1.1	Overview	13
1.2	LINX-100 / LINX-101	15
1.3	M-Bus	16
1.4	Modbus.....	16
1.5	Scope.....	16
2	Quick-Start Guide	17
2.1	Hardware Installation.....	17
2.2	Configuration of the LINX-10X	17
2.2.1	IP Configuration on the Console	18
2.2.2	IP Configuration via the Web Interface	19
2.3	Configuration with LNS-based Tools.....	20
2.4	Connect with an OPC XML-DA Client	24
3	Hardware Installation	25
3.1	Enclosure	25
3.1.1	LINX-10X.....	25
3.2	Product Label.....	26
3.3	Mounting.....	26
3.4	LED signals.....	26
3.4.1	Power LED	26
3.4.2	Status LED.....	26
3.4.3	OPC LED.....	26
3.4.4	FT Activity LED.....	27
3.4.5	Ethernet Link LED.....	27
3.4.6	Ethernet Activity LED	27
3.4.7	CNIP LED	27
3.4.8	CS/RNI LED.....	28
3.4.9	Wink Action.....	28
3.4.10	Network Diagnostics.....	28
3.5	Status Button	28
3.5.1	Resetting Forwarding Tables	29
3.6	DIP Switch Settings.....	29
3.7	Terminal Layout and Power Supply	29
3.8	Wiring	30
4	Web Interface	31

4.1	Device Information and Account Management	31
4.2	Device Configuration.....	33
4.2.1	System Configuration.....	33
4.2.2	Backup and Restore.....	34
4.2.3	Port Configuration.....	35
4.2.4	IP Configuration.....	35
4.2.5	CEA-709 Configuration	37
4.2.6	CEA-852 Device Configuration.....	37
4.2.7	CEA-709 Router Configuration	39
4.2.8	CEA-852 Server Configuration.....	39
4.2.9	CEA-852 Channel List	41
4.2.10	E-mail Configuration.....	42
4.2.11	Data Points	43
4.2.12	Trend	45
4.2.13	Scheduler	46
4.2.14	Calendar	48
4.2.15	Alarm.....	49
4.3	Device Statistics	49
4.3.1	IP Statistics.....	50
4.3.2	CEA-852 Statistics	50
4.3.3	Enhanced Communications Test	51
4.3.4	CEA-709 Statistics	52
4.3.5	System Log.....	52
4.3.6	OPC Server Statistics Page.....	53
4.3.7	Scheduler Statistics Page.....	54
4.3.8	Alarm Log Page	55
4.4	L-WEB.....	56
4.5	Reset, Contact, Logout.....	56
5	Concepts	58
5.1	CEA-709 OPC Server.....	58
5.2	Data Points	59
5.2.1	Overview	59
5.2.2	Timing Parameters	59
5.2.3	Default Values.....	60
5.2.4	Persistency.....	60
5.2.5	Behavior on Value Changes	60
5.2.6	Custom Scaling	61
5.2.7	System Registers	61
5.2.8	User Registers	61

5.2.9	Math Objects.....	61
5.3	Connections	62
5.4	AST Features	62
5.4.1	Alarming.....	62
5.4.2	Historical Alarm Log.....	63
5.4.3	Scheduling	63
5.4.4	Trending.....	66
5.4.5	E-mail	66
5.5	CEA-709 Technology	67
5.5.1	CEA-709 Data Points.....	67
5.5.2	Static Interface Changes	68
6	The LINX-10X Configurator.....	69
6.1	Installation	69
6.1.1	Software Installation	69
6.1.2	Registration as a Plug-In.....	69
6.1.3	Operating Modes	71
6.2	Data Point Manager.....	71
6.2.1	Folder List.....	71
6.2.2	Network Port Folders.....	72
6.2.3	Data Point List	73
6.2.4	Property View	74
6.2.5	Managing Multistate Maps	75
6.2.6	CEA-709 Properties.....	76
6.3	Project Settings.....	78
6.3.1	General.....	78
6.3.2	Data Point Naming Rules.....	79
6.3.3	CEA-709 Settings	79
6.3.4	AST Settings.....	80
6.3.5	Device Configuration.....	82
6.4	Workflows for the LINX-10X.....	82
6.4.1	Involved Configuration Files.....	83
6.4.2	Configure with LNS	83
6.4.3	Configure without LNS	84
6.4.4	Configure without LNS Using Bindings	84
6.4.5	Replace a LINX-10X.....	85
6.5	Adding LINX-10X.....	86
6.6	Replace a LINX-10X.....	89
6.7	Using the LINX-10X Configurator.....	92
6.7.1	Starting as an LNS Plug-In	92

6.7.2	Starting Stand-Alone	92
6.7.3	Uploading the Configuration	93
6.7.4	Scanning for Network Variables	94
6.7.5	Importing Network Variables	95
6.7.6	Scanning NVs online from the Network	96
6.7.7	Select and Use Network Variables	99
6.7.8	Change the NV Allocation	99
6.7.9	Create Static NVs	100
6.7.10	Create External NVs	101
6.7.11	Create User Registers	103
6.7.12	Configuration Download	104
6.7.13	Build XIF for Port Interface	105
6.7.14	Enable Legacy NM Mode	105
6.7.15	Upload Dynamic NVs from Device	106
6.7.16	Upload the System Log	106
6.8	Advanced CEA-709 Configuration	107
6.8.1	Import Devices from XIF Templates	107
6.8.2	Install Unconfigured Devices	108
6.8.3	Using Feedback Data Points	109
6.8.4	Working with Configuration Properties	110
6.8.5	Working with UNVTs, UCPTs	111
6.9	Connections	111
6.9.1	Create a New Connection	111
6.9.2	Create Connections from a CSV File	113
6.9.3	Modify Connections	113
6.9.4	Connection Overview	114
6.10	E-mail Templates	114
6.10.1	Create an E-mail Template	114
6.10.2	Trigger E-mails	115
6.10.3	Attachments	116
6.10.4	Limit E-mail Send Rate	117
6.11	Local Schedule and Calendar	117
6.11.1	Create a local Calendar	117
6.11.2	Create Calendar Pattern	118
6.11.3	Create a Local Scheduler	118
6.11.4	Configure Scheduled Data Points	119
6.11.5	Configure Daily Schedules	120
6.11.6	Configure Exception Days	122
6.11.7	Configure Embedded Exceptions	123

6.11.8 Configure Control Data Points	124
6.11.9 Using the SNVT_tod_event.....	124
6.11.10 Using the Local Scheduler	125
6.11.11 Limitations for Local CEA-709 Schedulers	125
6.12 Local Alarming.....	125
6.12.1 Create an Alarm Server.....	125
6.12.2 Create an Alarm Condition	126
6.12.3 Deliver Alarms via E-mail	128
6.12.4 Create an Alarm Log.....	129
6.12.5 Limitations for CEA-709 Alarm Servers	130
6.13 Local Trending	130
6.13.1 Create a Local Trend.....	130
6.13.2 Configure Trended Data Points	131
6.13.3 Trend Triggers	132
6.13.4 Download Trend Data in CSV Format	133
6.13.5 Deliver Trend Data via E-mail.....	133
6.13.6 Limitations for Local CEA-709 Trends.....	134
6.14 Remote AST Objects.....	134
6.14.1 Remote Scheduler and Calendar	134
6.14.2 Alarm Clients.....	135
6.15 Math Objects	136
6.15.1 Create a Math Object	136
6.15.2 Editing a Math Object.....	137
7 The LINX-101 Router	139
7.1 CEA-709 Router.....	139
7.1.1 Configured Router Mode	140
7.1.2 Smart Switch Mode	140
7.1.3 Store-and-Forward Repeater.....	141
7.1.4 Smart Switch Mode with No Subnet Broadcast Flooding	141
7.2 CEA-852 Device of the Router	141
7.3 Configuration Server for Managing the IP-852 Channel.....	142
7.3.1 Overview.....	142
7.3.2 Configuration Server Contacts IP-852 Device	143
7.3.3 IP-852 Device Contacts Configuration Server	143
7.3.4 Using the Built-In Configuration Server.....	144
7.4 Firewall and NAT Router Configuration	144
7.4.1 Automatic NAT Configuration	144
7.4.2 Multiple IP-852 Devices behind a NAT: Extended NAT Mode	145
7.4.3 Multiple IP-852 devices behind a NAT: Classic Method	147

7.5	Multi-Cast Configuration	148
7.6	Remote LPA Operation.....	149
7.7	Internet Timing Aspects.....	150
7.7.1	Channel Timeout	150
7.7.2	Channel Delay	150
7.7.3	Escrowing Timer (Packet Reorder Timer)	151
7.7.4	SNTP Time Server	151
7.8	Advanced Topics.....	151
7.8.1	Aggregation	151
7.8.2	MD5 Authentication.....	151
7.8.3	Dynamic NAT Addresses.....	152
8	The LINX-100 RNI.....	153
8.1	RNI Function	153
8.2	Remote LPA Operation.....	153
9	OPC Server	155
9.1	XML-DA OPC Server	155
9.1.1	Access Methods.....	155
9.1.2	Data Points	156
9.1.3	AST Objects	159
9.2	Using L-WEB.....	161
9.2.1	Create a new L-WEB Project	162
9.2.2	Start a Graphical L-WEB Design.....	163
9.2.3	Organize L-WEB Projects.....	163
9.3	Using the OPC Bridge.....	164
9.3.1	Software Installation	164
9.3.2	Configure the Bridge Locally.....	165
9.3.3	Export OPC Servers for another PC.....	165
9.3.4	Import OPC Servers Using the Configurator	166
9.3.5	Manually Configure Servers	166
9.3.6	Bridge Timing Parameters.....	167
9.4	Using Custom Web Pages	168
10	M-Bus	169
10.1	Introduction	169
10.2	Hardware Installation	169
10.3	M-Bus Network.....	169
10.4	Web Interface.....	170
10.4.1	Configuration	170
10.4.2	Data Points	170
10.4.3	Statistics	170

10.4.4 M-Bus Protocol Analyzer	171
10.5 Configurator	172
10.5.1 Activating M-Bus Configuration	172
10.5.2 Data Point Manager for M-Bus	172
10.5.3 Folder List.....	173
10.5.4 Network Port Folders.....	174
10.5.5 M-Bus Properties	174
10.5.6 M-Bus Workflow.....	175
10.5.7 Using the Configurator for M-Bus.....	176
11 Modbus	192
11.1 Introduction.....	192
11.2 Modbus Network.....	192
11.3 Web Interface.....	193
11.3.1 Port Configuration	193
11.3.2 Data Points.....	194
11.3.3 Statistics	194
11.3.4 Modbus Protocol Analyzer	195
11.4 Configurator.....	195
11.4.1 Activating Modbus Configuration	195
11.4.2 Data Point Manager for Modbus	196
11.4.3 Folder List.....	197
11.4.4 Network Port Folders.....	198
11.4.5 Modbus Properties	198
11.4.6 Modbus Workflow.....	198
11.4.7 Using the Configurator for Modbus.....	199
12 Operating Interfaces	212
12.1 Common Interface	212
12.1.1 Schedule and Calendar XML Files.....	212
12.1.2 Trend Log CSV File	212
12.1.3 Alarm Log CSV File.....	213
12.2 CEA-709 Interface	214
12.2.1 NV Import File.....	214
12.2.2 Node Object.....	215
12.2.3 Real-Time Keeper Object	216
12.2.4 Channel Monitor Object	216
12.2.5 Calendar Object	218
12.2.6 Scheduler Object.....	218
12.2.7 Clients Object	218
12.2.8 Gateway Objects.....	218

13 Network Media	219
13.1 FT	219
13.2 M-Bus	220
13.3 Modbus RS-485.....	220
14 LINX-10X Firmware Update	221
14.1 Firmware Update via the LINX-100/200 Configurator	221
14.2 Firmware Update via the Console.....	223
15 Troubleshooting.....	225
15.1 Technical Support	225
15.2 Statistics on the Console.....	225
15.2.1 Connecting to the Console	225
15.2.2 Reset configuration (load factory defaults)	226
15.2.3 Device Statistics Menu	226
16 Application Notes	229
16.1 The LSD Tool.....	229
16.2 Use of Static, Dynamic, and External NVs on a Device	229
17 Firmware Versions	230
18 Specifications	231
18.1 LINX-10X.....	231
18.1.1 Physical Specifications.....	231
18.1.2 Resource Limits.....	231
19 References	233
20 Revision History	234

Abbreviations

100Base-T	100 Mbps Ethernet network with RJ-45 plug
Aggregation	Collection of several CEA-709 packets into a single CEA-852 packet
AST	Alarming, Scheduling, Trending
BOOTP	Bootstrap Protocol, RFC 1497
CEA-709	Protocol standard for LONWORKS networks
CEA-852	Protocol standard for tunneling CEA-709 packets over IP channels
COV	change-of-value
CR	Channel Routing
CS	Configuration Server that manages CEA-852 IP devices
DA	Data Access (Web service)
DHCP	Dynamic Host Configuration Protocol, RFC 2131, RFC 2132
DIF, DIFE	Data Information Field, Data Information Field Extension
DL	Data Logger (Web service)
DNS	Domain Name Server, RFC 1034
DST	Daylight Saving Time
GMT	Greenwich Mean Time
IP	Internet Protocol
IP-852	logical IP channel that tunnels CEA-709 packets according CEA-852
LSD Tool	LOYTEC System Diagnostics Tool
MAC	Media Access Control
MD5	Message Digest 5, a secure hash function, see Internet RFC 1321
M-Bus	Meter-Bus (Standards EN 13757-2, EN 13757-3)
NAT	Network Address Translation, see Internet RFC 1631
NV	Network Variable
OPC	Open Process Control
PLC	Programmable Logic Controller
RNI	Remote Network Interface
RTT	Round-Trip Time
RTU	Remote Terminal Unit
SL	Send List
SMTP	Simple Mail Transfer Protocol
SNTP	Simple Network Time Protocol
SNVT	Standard Network Variable Type
SSL	Secure Socket Layer
TLS	Transport Layer Security
UI	User Interface
UNVT	User-defined Network Variable Type
VIF, VIFE	Value Information Field, Value Information Field Extension
XML	eXtensible Markup Language

1 Introduction

1.1 Overview

The LINX-10X is a high performance, reliable, and secure network infrastructure component that contains an embedded OPC server and exposes a defined set of data points as OPC tags. It implements the OPC XML-DA standard, which lets OPC clients access the data points via Web services. The LINX-10X can provide up to 1000 OPC tags. Which native data points are exposed to OPC can be configured by a configuration software, which provides a fast and easy way to configure the LINX-10X. Using the supplied L-Web designer, users can easily generate a Web-based visualization for the LINX-10X. Easy to understand diagnostic LEDs allow installers and system integrators to install and troubleshoot this device without expert knowledge and dedicated troubleshooting tools.

The CEA-709 OPC Server (LINX-100, LINX-101) is equipped with an FT port (CEA-709) and a 100Base-T Ethernet port (CEA-852) and exposes CEA-709 network variables (NVs) and configuration properties (CPs) to the OPC world. The configuration software can be run as LNS plug-in or stand-alone. The OPC server node is connected to the FT port. The LINX-101 also contains a router between the FT and the IP-852 channel, which can be configured like an L-IP. It includes a configuration server (CS) to manage the IP-852 channel. The LINX-100 contains a remote network interface (RNI) instead of the router for remote network access. The device is fully compliant with ANSI/CEA-709, ANSI/CEA-852-A, EN 14908, and OPC XML-DA 1.01.

The OPC server's NVs can be bound in the CEA-709 network or operated as "external NVs". External NVs are polled or explicitly written to without allocating static or dynamic NVs on the LINX-10X. In this case, address information is supplied by the configuration software by importing e.g., a CSV file. User-defined network variable types (UNVTs) can be used as dynamic or external NVs. Configuration properties (CPs) on other devices can be accessed through file transfer. To transfer CPs, the device supports both the LONMARK file transfer and the read memory access method. For CPs, the standard SCPTs and user-defined UCPTs are supported. All those CEA-709 data points can be exposed as OPC tags. The LINX-10X also supports the M-Bus interface according to EN 13757-2, EN 13757-3. M-Bus data points can be connected to CEA-709 NVs and exposed to OPC. Additionally a Modbus RTU (Remote Terminal Unit) and a Modbus TCP interface is supported by the LINX-10X. Also the Modbus data points can be exposed to OPC and connected to CEA709-NVs, BACnet objects and register data points.

The LINX-10X also supports the LOYTEC Alarming, Scheduling and Trending (AST) feature set. The device provides LONMARK scheduler/calendar objects, which can directly schedule NVs or registers. For alarm conditions, the LINX-10X can be configured to send e-mails to predefined addresses. Alarms can also be stored in a historical *alarm log*. There can be up to 100 trend log objects with an aggregated total log buffer size of 2MB. The LINX-10X provides mathematics objects, which can be used to combine data points using a mathematical formula. The AST objects are exposed to a set of OPC tags. Trend logs can

be uploaded from the device in CSV format. In addition, a dedicated Web service can be used to access trend log information.

The LINX-10X permanently collects statistical information from the attached network channels (channel load, CRC errors, forwarding statistics, etc.). Using this data, the LINX-10X software is able to detect problems on these channels (overload, connections problems, etc.) and warns the system operator via LEDs (see Section 3.4.10). An intuitive user interface allows fast and easy network troubleshooting without any additional analysis tools or deep system knowledge. The LSD Tool can be used for a more detailed view of the collected statistics data. See Section 16.1 for more information on this powerful system diagnostics tool. The LINX-10X also includes channel monitoring objects for the FT and the IP-852 channel, which make the channel statistics available through NVs. The channel statistics is also exposed to the OPC interface.

The built-in Web server allows convenient device configuration through a standard Web browser such as the Internet Explorer or Firefox. The Web interface also provides statistics information for system installation and network troubleshooting.

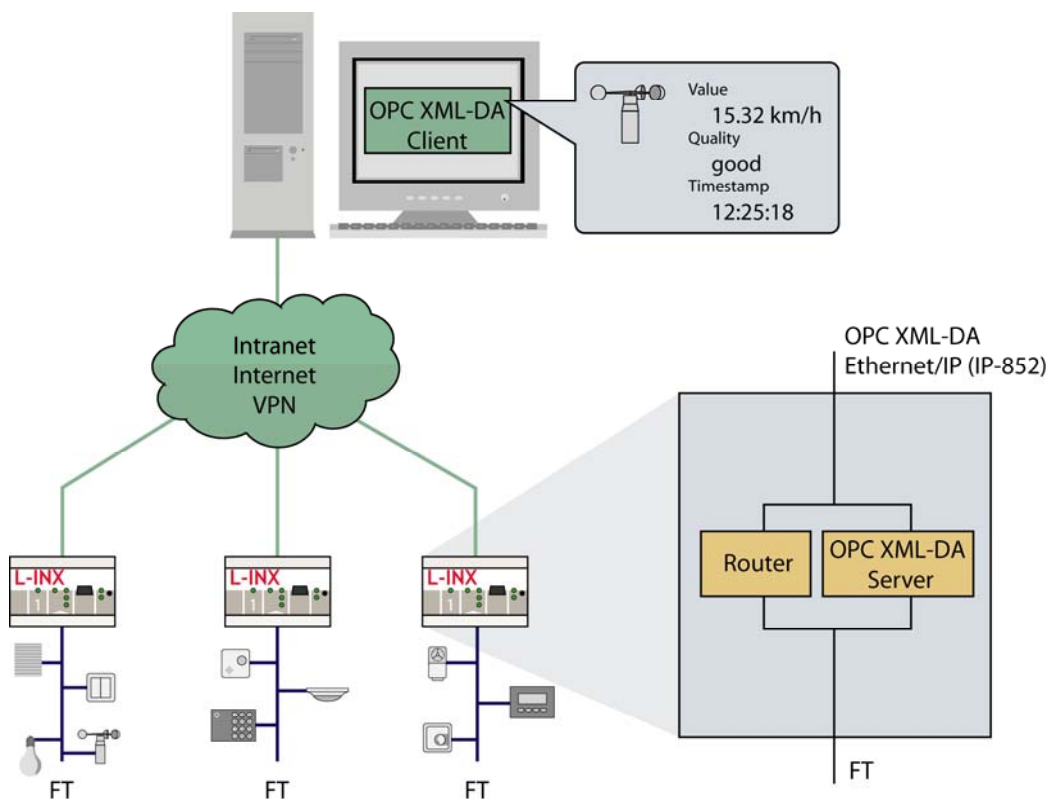


Figure 1: LINX-10X application example with an IP-852 channel.

The LINX-10X is used for:

- Exposing CEA-709 network variables (NVs) and configuration properties (CPs) as OPC tags,
- visualization of a CEA-709 network with the supplied LOYTEC L-Web software,
- visualization of a CEA-709 network in an OPC XML-DA SCADA package,
- automatic meter reading applications via CEA-709, M-Bus and Modbus,
- reading, writing, and subscribing to CEA-709 NVs and CPs via Web services (.NET),
- building custom Web pages with active content,
- browsing data points on the Web interface,

- supporting standard (SNVT, SCPT) and user-defined (UNVT, UCPT) types,
- scheduling CEA-709 network variables,
- trending data points,
- generating alarms,
- logging alarms,
- sending e-mails on alarms, trend logs, or scheduled events,
- CEA-709 PC applications (as a CEA-709 network interface),
- remote LPA functionality,
- communicating on CEA-709 with either FT or IP-852 (IP channel on the Intranet/Internet),
- connecting an FT channel to a high-performance backbone using existing IP infrastructure,
- operating as a configuration server for IP-852 devices.

1.2 LINX-100 / LINX-101

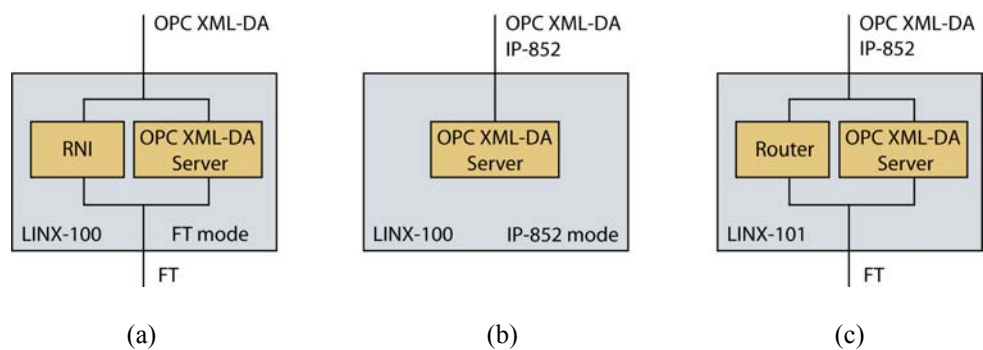


Figure 2: LINX-100 (a, b) versus LINX-101 (c).

The LINX-100 and the LINX-101 are both capable of exposing CEA-709 network variables and configuration properties to OPC XML-DA. Depending on additional features, there are different flavors of the product. Figure 2 depicts the differences.

The LINX-101 possesses a router between the CEA-852 interface (IP-852) and the FT interface. The built-in router can be used behind NAT routers and firewalls, which allows seamless integration in already existing Intranet networks. It supports DHCP even with changing IP addresses in an Intranet environment. The CEA-852 interface can be used to connect the LINX-101 to an IP-based high-speed backbone. The LINX-101's router can be used as a standard CEA-709 configured router or it can be used as a self-learning plug&play router based on the high-performance, well-proven routing core from our L-Switch plug&play multi-port router devices ("smart switch mode"). The self-learning router doesn't need a network management tool for configuration but is a true plug&play and easy to use IP infrastructure component.

The LINX-100 can be configured to run either on the CEA-852 interface (IP-852 mode) or on the FT interface (FT mode). In the FT mode, the device provides a remote network interface (RNI), which appears like a LOYTEC NIC-IP is intended to be used together with the LOYTEC NIC software [2]. The RNI can be utilized for remote access and configuration as well as trouble-shooting with the remote LPA. Please consult our product literature for the LPA-IP to learn more about this IP-based CEA-709 protocol analyzer.

1.3 M-Bus

In addition to the basic network technologies above, this device supports the M-Bus interface according to the standards EN 13757-2 and EN 13757-3. To gain access to the M-Bus network, an external M-Bus interface must be attached to the device's serial connector. The user can turn M-Bus support on and off via a DIP switch on the device.

Through the M-Bus interface the device can be used to scan the attached M-Bus network for devices, pull M-Bus data points into a configuration, connect those data points to other technologies, and expose M-Bus data points to OPC tags. All AST functions can be used directly on M-Bus data points. Especially trending data and polling for data on M-Bus devices has been optimized for automatic meter reading applications.

For debugging purposes a protocol analyzer is included in the firmware.

For more information on how to set up the device for using M-Bus, configuring and using M-Bus data points, refer to Chapter 10.

1.4 Modbus

In addition to the basic network technologies above, this device supports the Modbus RTU and the Modbus TCP interface. To gain access to the Modbus network, the appropriate interfaces have to be activated either in the console user interface or in the web UI. Modbus RTU is operated with 8N1. A Modbus port can either be operated as Modbus master or Modbus slave.

Through the Modbus interface the device can be used to connect data points to other technologies, and expose Modbus data points to OPC tags. All AST functions can be used directly on Modbus data points. Especially trending data and polling for data on Modbus devices has been optimized for automatic meter reading applications.

For debugging purposes a protocol analyzer is included in the firmware.

For more information on how to set up the device for using Modbus, configuring and using Modbus data points, refer to Chapter 11.

1.5 Scope

This document covers LINX-10X devices with firmware version 3.5 and the LINX-10X Configurator version 3.5 and higher. See Section 17 for differences between the different LINX-10X firmware versions.

2 Quick-Start Guide

This chapter shows step-by-step instructions on how to configure the LINX-10X for a simple OPC server application.

2.1 Hardware Installation

Connect power (12-35 VDC or 12-24 VAC), the CEA-709 network, and the Ethernet cable as shown in Figure 3. More detailed instructions are shown in Chapter 3.

Important: *Do not connect terminal 17 with Earth-ground!*

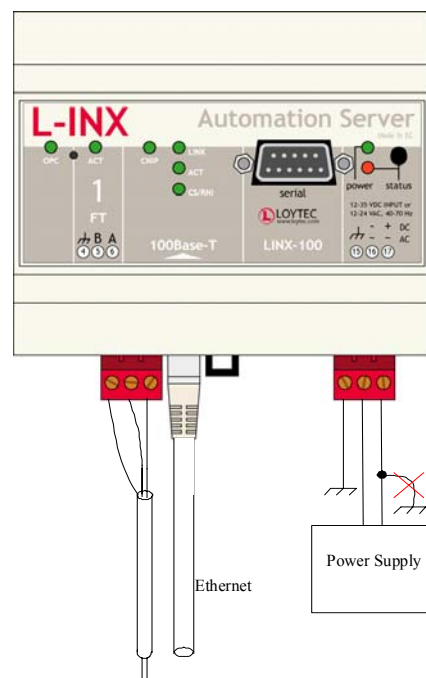


Figure 3: Basic Hardware Installation.

2.2 Configuration of the LINX-10X

The LINX-10X can be configured via a console interface or via the Web interface. To configure the LINX-10X, the following steps have to be performed:

1. Setup IP configuration (see Sections 2.2.1 and 2.2.2).

2. Setup the OPC configuration (see Section 2.3).

Note: This setup procedure assumes the use of the IP interface.

2.2.1 IP Configuration on the Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. To connect COM1 of the PC to the Console on the LINX-10X, use a standard null-modem cable with full handshaking. Power up the LINX-10X or press **Return** if the LINX-10X is already running. The following menu should appear on the terminal:

```
Device Main Menu
=====
[1] Show device information
[2] Serial firmware upgrade
[3] System configuration
[4] CEA-709 configuration
[5] IP configuration
[6] CEA-852 device configuration
[7] CEA-852 server configuration
[8] Reset configuration (factory defaults)
[9] Device statistics

[a] Data Points
[0] Reset device

Please choose:
```

Figure 4: LINX-101 Main Menu.

Select '5' from the LINX-10X Configuration Menu and enter the IP address, netmask, and gateway address. Note that you must use different IP addresses if you are using multiple LINX-10X in your setup.

```
IP Configuration Menu
=====
[1] DHCP : disabled
[2] IP Address : 192.168.24.99
[3] IP Netmask : 255.255.192.0
[4] IP Gateway : 192.168.1.1
[5] Hostname : test-linx101
[6] Domainname : <unset>
[7] DNS Servers : 10.101.17.2
[9] MAC Address : 00:0A:B0:01:0A:4C (factory default)
[0] NTP Servers : <unset> (out-of-sync)
[b] Link Speed & Duplex : Auto Detect

[q] Quit without saving
[x] Exit and save

Please choose:
```

Figure 5: Enter basic IP settings.

Press 'x' to save the IP settings and reset the LINX-10X with the main menu item '0' in order to let the new IP settings take effect.

Important! *The default IP address 192.168.1.254 is only set for configuration access. It must be changed in order to make the device functional.*

You should now be able to connect to the LINX-10X with a Web browser and add the LINX-101's router to an IP-852 channel in the configuration server member list. If the LINX-101 should also act as the configuration server please proceed to Section 4.2.8.

2.2.2 IP Configuration via the Web Interface

Optionally to using the console interface one can also use the Web interface to configure the client device. In a Web browser enter the default IP address '192.168.1.254' of the LINX-10X. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx, please open a command tool and enter the following route command to add a route to the LINX-10X.

To Add a Route to the Device

1. Windows **START** → **Run**
2. Enter 'cmd' and click **OK**.
3. In the command window enter the command line
`route add 192.168.1.254 %COMPUTERNAME%`
4. Then open your Web browser and type in the default IP address 192.168.1.254.

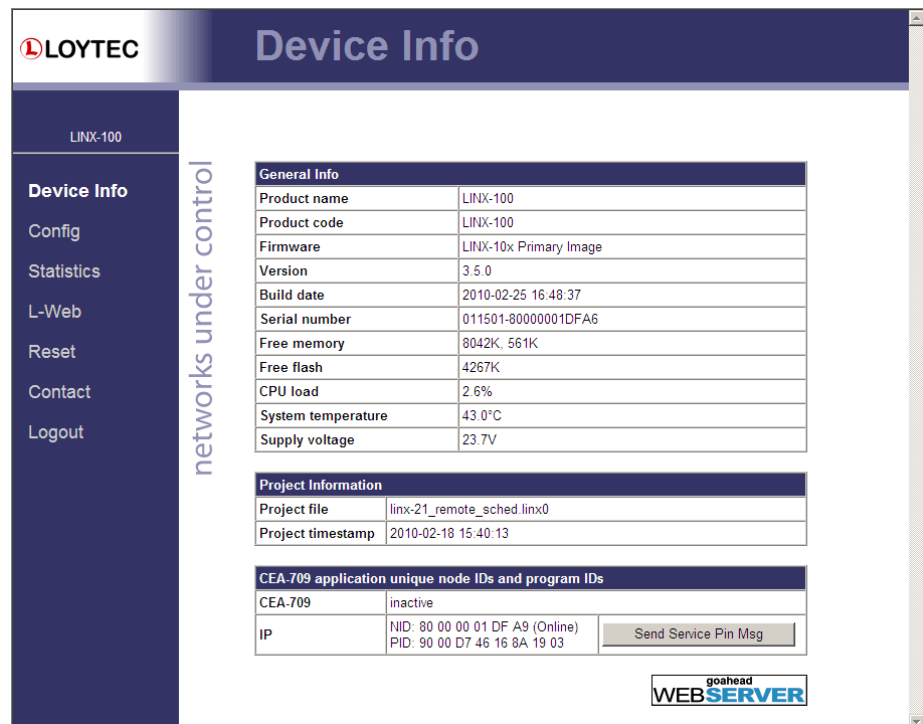


Figure 6: Example Start Screen.

5. Click on **Config** in the left menu. You will be asked to enter the administrator password in order to change the IP settings. Enter 'admin' and select **Login**.

Figure 7: Enter 'admin' as the default administrator password.

- The Config menu opens. Click on **Port Config** and change to the tab Ethernet. The TCP/IP settings are selected as shown in Figure 8. Enter the IP address, the IP netmask, and IP gateway for this LINX-10X.

Figure 8: Enter IP address and gateway.

- Press **Save Settings** and then reset the device by selecting **Reset** in the highlighted text. This changes the IP settings of the LINX-10X.

2.3 Configuration with LNS-based Tools

This section describes a quick start scenario for the LINX-10X. In this scenario, network variables of nodes connected to the FT port shall be exposed as OPC tags. As a network management tool, an LNS-based tool is used.

First, install the LINX-100/200 Configurator Software from the “setup.exe”. This file can be downloaded from www.loytec.com. In your LNS-based tool, register the LINX-100/200 Configurator as LNS plug-in.

Then open an LNS database and add a LINX-10X device using the device template for the LINX-10X (LINX-10x_FT-10). Configure the added device with the LINX-100/200 Configurator plug-in. This opens the data point manager screen of the software as shown in Figure 9. Note that the device status is displayed as “Configured” on the right-hand side below the speed button bar.

Click on the **Scan Channel** speed button marked by the red rectangle in Figure 9 to scan all NVs found on nodes connected to the LINX-10X’s FT channel. Figure 10 shows an example result of the scan. Now select the NVs which shall be exposed as OPC tags and click on the **Use on Device** speed button as marked by the red rectangle in Figure 10.

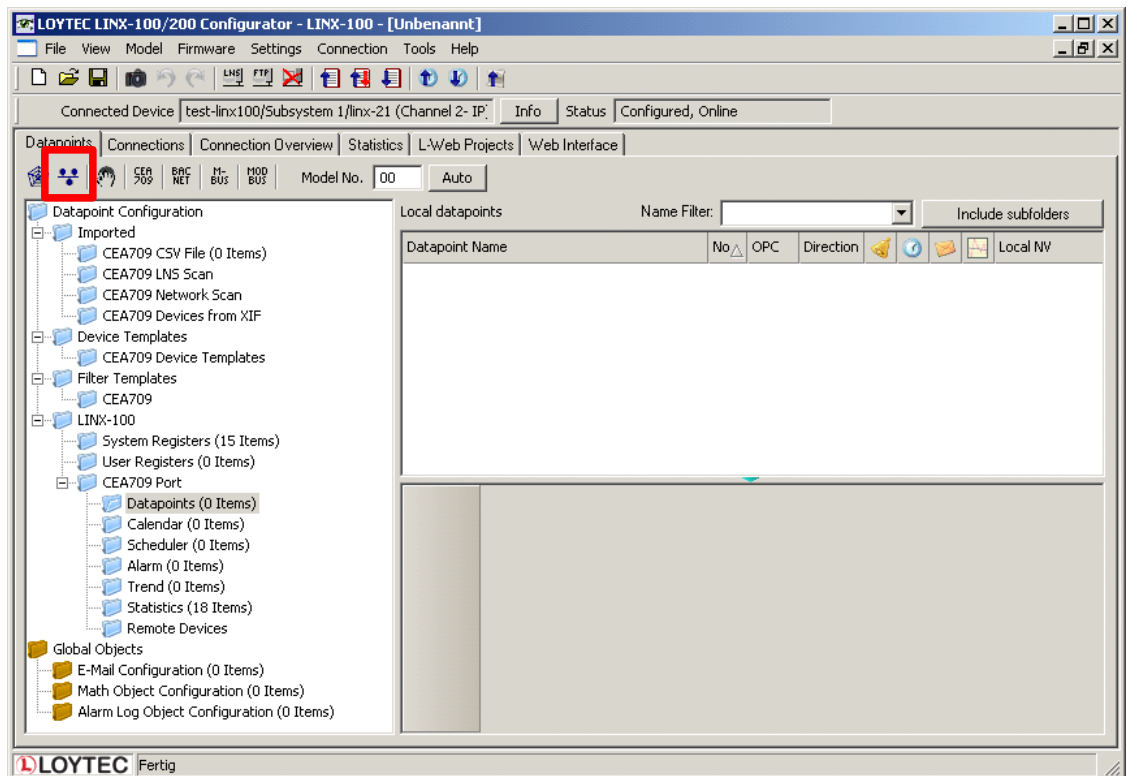


Figure 9: LINX-100/200 Configurator main screen.

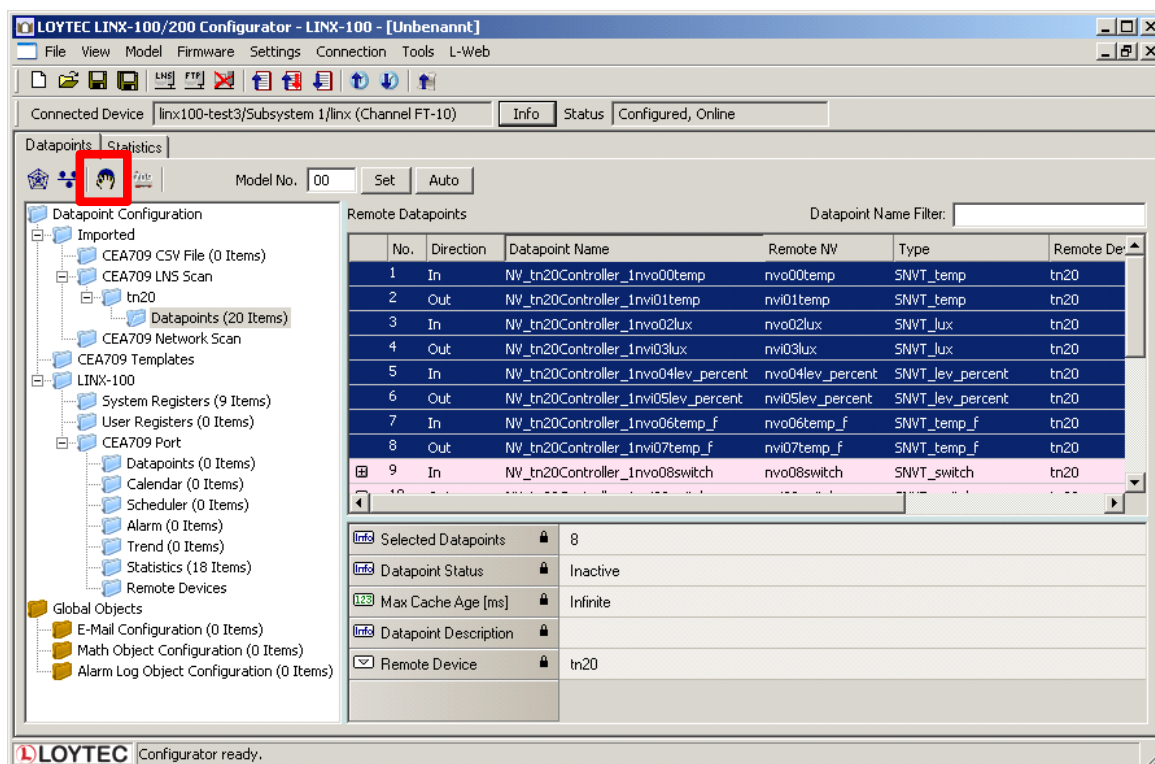


Figure 10: Example result of scanned NVs from LNS channel.

The data points now appear in the LINX-10X device folder as shown in Figure 11. The data point name will be used as the name of the OPC tag. Now click on the **Download Configuration** speed button as indicated by the red rectangle in Figure 11. The Configurator will require saving the project file to the hard drive. Select a file name and save the file.

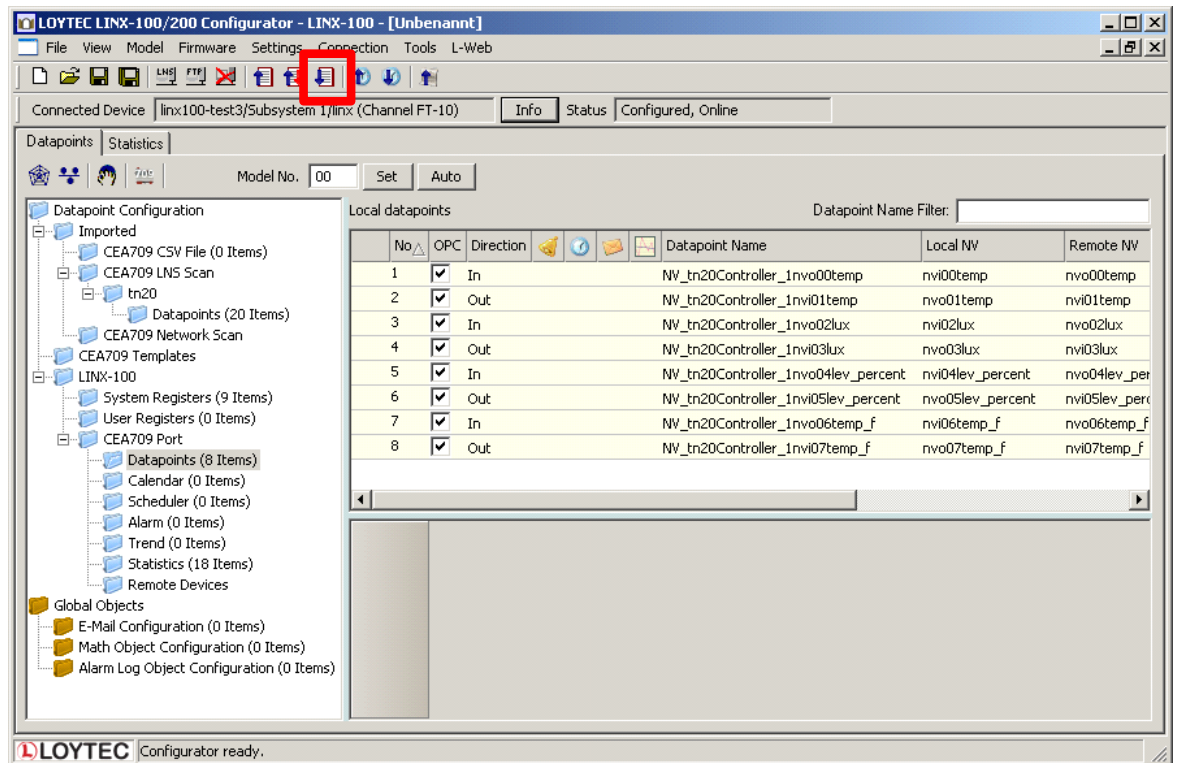


Figure 11: NVs used for OPC tags on the LINX-10X.

Then the **Configuration Download** dialog opens as depicted in Figure 12. Press **Start**. The tasks executed are displayed and their progress is visualized by the progress bar below.

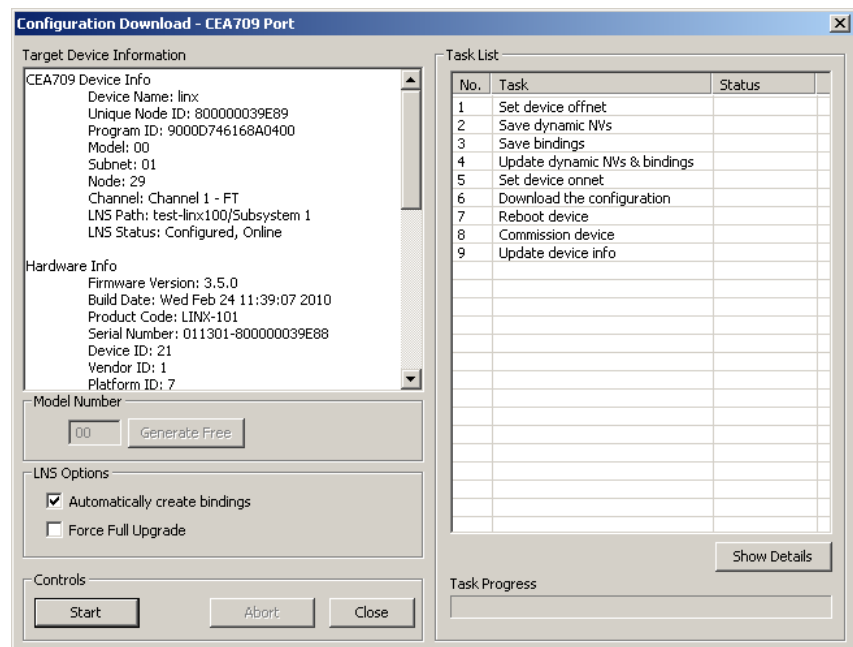


Figure 12: Configuration Download Dialog.

When the configuration process is complete, a dialog box is shown, which must be acknowledged by clicking **OK**. Then the LINX-10X is up and running with the new configuration. To verify the configuration, go to the LINX-10X's Web interface and click on **Config** and **OPC Data Points**, which brings up the Web page as shown in Figure 13. The list displays current data point values and status.

LOYTEC Data Points

LINX-101
Logged in as
admin

Device Info

Config

- System
- Passwords
- Backup/Restore
- Port Config
- CEA-709 Router
- CEA-852 Server
- CEA-852 Ch. List
- E-mail
- Data Points**
 - Trend
 - Scheduler
 - Calendar
 - Alarm

Statistics

networks under control

ROOT

- System Registers
- User Registers
- CEA709 Port
 - Datapoints
 - tn50
 - Calendar
 - Scheduler
 - Alarm
 - Trend
 - Statistics
 - Remote Devices
 - CEA852 Port

Reload

Folder: /CEA709 Port/Datapoints/tn50/

Name	Dir.	Type	Value	State
NV_tn50Controller_1nvo00temp	input	analog	-273.2	normal
NV_tn50Controller_1nvo01temp	output	analog	--	invalid value
NV_tn50Controller_1nvo02lux	input	analog	8	normal
NV_tn50Controller_1nvo03lux	output	analog	--	invalid value
NV_tn50Controller_1nvo04lev_percent	input	analog	0.8	normal
NV_tn50Controller_1nvo05lev_percent	output	analog	--	invalid value
NV_tn50Controller_1nvo06temp_f	input	analog	0.800000071525574	normal
NV_tn50Controller_1nvo07temp_f	output	analog	--	invalid value
NV_tn50Controller_1nvo08switch	input	user	0000	normal
value	input	analog	0	normal
state	input	multistate	0	normal
NV_tn50Controller_1nvo09switch	output	user	--	invalid value
value	output	analog	--	invalid value
state	output	multistate	--	invalid value

Figure 13: Verify the data point configuration on the Web interface.

Note that the auto-generation created dynamic NVs as counterparts to the scanned NVs on the CEA-709 network and also created bindings for those NVs. If static NVs or external NVs (with polling) shall be used on the CEA-709 network or more advanced NV selection schemes shall be employed, please refer to Chapter 5 to learn more about the Configurator software.

2.4 Connect with an OPC XML-DA Client

After the configuration has been downloaded to the LINX-10X it is ready to serve OPC XML-DA clients. Connect to the LINX-10X using the URL

<http://192.168.24.99/DA>,

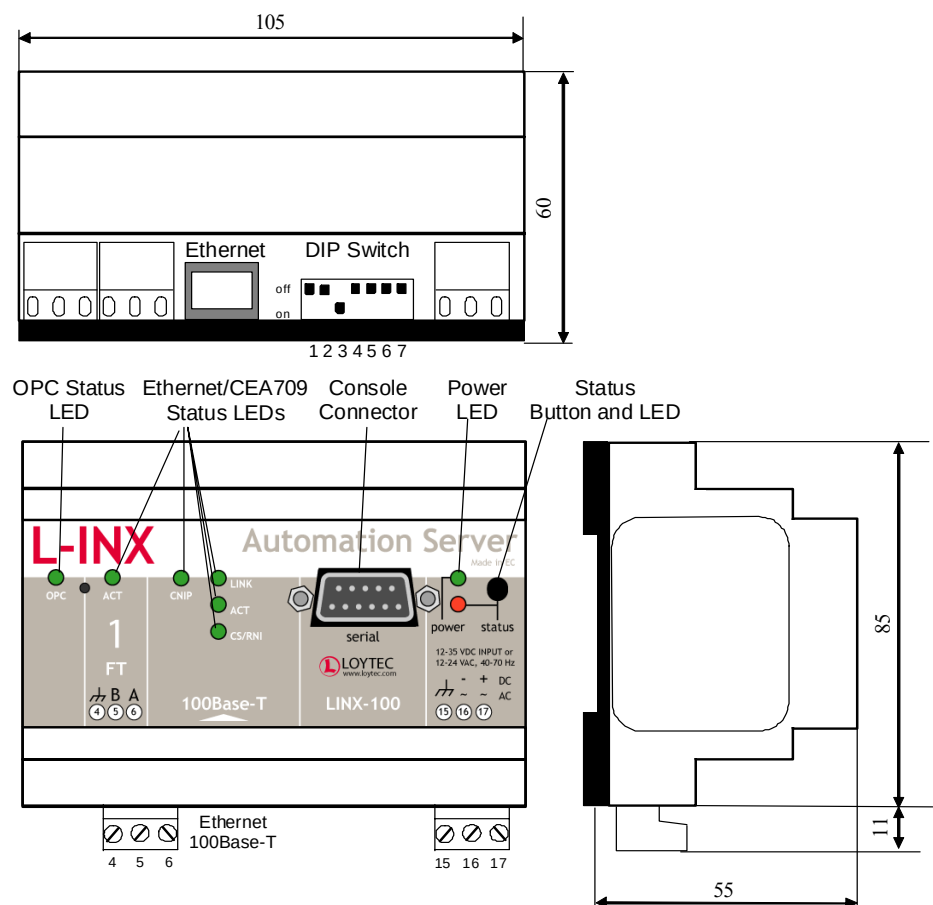
given that 192.168.24.99 is the IP address of the LINX-10X. Note, that by default, writing to OPC tags needs basic HTTP authentication using the password for the operator user. This is 'operator' by default.

3 Hardware Installation

3.1 Enclosure

3.1.1 LINX-10X

The LINX-10X enclosure is 6 TE (1 TE = 17.5 mm) wide for DIN rail mounting, following DIN 43 880 (see Figure 14).



3.2 Product Label

The product label on the side of the LINX-10X contains the following information (see Figure 15):

- LINX-10X order number with bar-code (e.g., LINX-100, LINX-101),
- serial number with bar-code (Ser#),
- unique node ID and virtual ID of each port (NID1, VID1) with bar-code,
- Ethernet MAC ID with bar-code (MAC1).

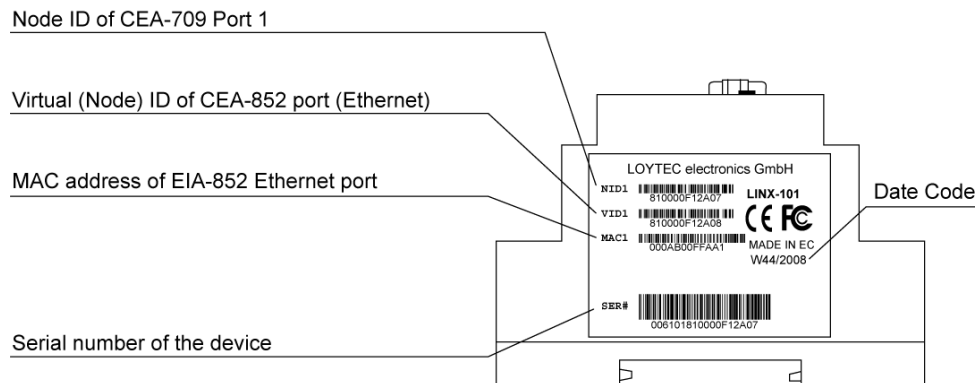


Figure 15: LINX-10X product label.

Unless stated otherwise, all bar codes are encoded using “Code 128”. An additional label is also supplied with the LINX-10X for documentation purposes. A virtual ID (VID) is a Node ID on the IP channel.

3.3 Mounting

The device comes prepared for mounting on DIN rails following DIN EN 50 022. The device can be mounted in any position. However, an installation place with proper airflow must be selected to ensure that the LINX-10X’s temperature does not exceed the specified range (see Chapter 18).

3.4 LED signals

3.4.1 Power LED

The LINX-10X power LED lights up green when power is supplied to terminals 16 and 17.

3.4.2 Status LED

The LINX-10X is equipped with a red status LED (see Figure 14). This LED is normally off. During boot-up the status LED is used to signal error conditions (red). If the fall-back image is executed the status LED flashes red once every second.

3.4.3 OPC LED

The OPC Server LED illuminates green when at least one OPC client is connected to the OPC server. The LED flickers on OPC XML-DA traffic activity.

3.4.4 FT Activity LED

The FT port on the LINX-10X has a three-color LED (green, red, and orange, see Figure 14). Table 1 shows different LED patterns of the port and their meaning.

Behavior	Description	Comment
GREEN flashing fast	Traffic	
GREEN flashing at 1Hz	The OPC node or LINX-101's router port is unconfigured	On the LINX-101 this LED only stops flashing if both, node and router, are commissioned.
RED permanent	Port damaged	
RED flashing fast	Traffic with high amount of errors	
RED flashing at 1 Hz (all ports)	Firmware image corrupt	Please upload new firmware.
ORANGE permanent	Port disabled	e.g., using LSD Tool
ORANGE flashing fast	Traffic on port configured as management port	e.g., using LSD Tool

Table 1: CEA-709 Activity LED Patterns.

3.4.5 Ethernet Link LED

The Ethernet Link LED lights up green whenever an Ethernet cable is plugged-in and a physical connection with a switch, hub, or PC can be established.

3.4.6 Ethernet Activity LED

The Ethernet Activity LED lights up green for 6 ms whenever a packet is transmitted or received or when a collision is detected on the network cable.

3.4.7 CNIP LED

The CNIP LED is a three color LED that indicates different operating states of the LINX-10X's CEA-852 device.

Green: The CEA-852 device is fully functional and all CEA-852 configuration data (channel routing info, channel membership list, send list) are up-to-date.

Green flicker: If a valid CEA-709 packet is received or transmitted over the IP channel the CNIP LED turns off for 50 ms. Only valid CEA-709 IP packets sent to the IP address of the LINX-10X can be seen. Stale packets or packets not addressed to the LINX-10X are not seen.

Yellow: Device is functional but some configuration data is not up-to-date (device cannot contact configuration server but has configuration data saved in Flash memory)

Red: Device is non-functional because it was rejected from the CEA-852 IP channel or shut-down itself due to an internal error condition.

Off: Device is non-functional because the CEA-852 device has not started. This can be the case if the LINX-10X uses DHCP and it has not received a valid IP configuration (address) from the DHCP server.

Flashing red at 1 Hz: Device is non-functional because the CEA-852 device is started but has not been configured. Please add the device to a CEA-852 IP channel (register in configuration server).

Flashing green or orange at 1 Hz: The LINX-10X's CEA-709 side of the gateway has not been commissioned yet. The color indicates the CEA-852 IP channel status as described above.

3.4.8 CS/RNI LED

On the LINX-101 this LED indicates the status of the CEA-852 configuration server. If illuminated green, the configuration server is enabled.

On the LINX-100 this LED indicates the remote network interface (RNI) status. The LED is dark, if RNI is not supported by this device or the interface is not enabled. The LED is green, if the RNI is currently in use.

3.4.9 Wink Action

If the LINX-10X receives a wink command on any of its network ports, it shows a blink pattern on the CNIP and the CEA-709 activity LEDs. The CEA-709 activity and the CNIP LED turn green/orange/red (each 0.15 s). This pattern is repeated six times. After that, the CNIP LED flashes orange six times if the wink command was received on the IP channel or the CEA-709 activity LED flashes orange six times if the wink command was received on the CEA-709 channel. After that the LINX-10X LEDs resume their normal behavior.

3.4.10 Network Diagnostics

The LINX-10X provides simple network diagnostics via its CEA-709 activity LED:

If the LED does not light up at all, this port is not connected to any network segment or the connected network segment currently shows no traffic.

If the LED is flashing green, the network segment connected to this port is ok.

If the LED is flashing red, a potential problem exists on the network segment connected to this port. This state is referred to as overload condition.

A port overload condition occurs if

- the average bandwidth utilization of this port was higher than 70 %, or
- the collision rate was higher than 5 %, or
- more than 15 % CRC errors have occurred on a port with a power-line transceiver, or more than 5 % on a port with a transceiver other than power-line, or
- the LINX-10X was not able to process all available messages.

For a deeper analysis of the reason for the overload condition, it is recommended to use a protocol analyzer (e.g., LOYTEC's LPA) or a similar tool. The exact reason of the overload condition can also be determined with the LSD Tool.

3.5 Status Button

The LINX-10X is equipped with a status button (see Figure 14). When pressing the status button shortly during normal operation of the LINX-10X, it sends a "Service Pin Message" on the active CEA-709 network port (FT or CEA-852). As an alternative to pressing the status button, a service pin message can be sent via the Web interface (see Section 4.1).

The status button can also be used to switch the device back to factory default state. Press the service button and power-cycle the device. Keep the button pressed until the port LEDs illuminate orange permanently. Release the button within five seconds from that time on to reset the device to factory defaults. Alternatively, the device can be switched back to factory defaults over the console UI (see Section 15.2.2).

3.5.1 Resetting Forwarding Tables

In order to reset the forwarding tables of the LINX-10X's router, the status button needs to be pressed for at least 20 seconds during normal operation of the LINX-10X. Resetting forwarding tables means:

- Resetting the CEA-709 transceiver to the standard values.
- Setting all ports to unconfigured.
- Clearing the group forwarding, the subnet/node forwarding and the router domain table when used in smart switch mode.
- Clearing the LINX-10X status and statistic data.
- But **does not** clear the IP address, the CEA-852 configuration settings, and the data point configuration.

All this is done when the button is released. Afterwards a reset is performed to let the changes take effect.

Important:	<i>If the LINX-10X is moved from one location to another or if major changes to the configuration of the network are made, it is recommended to reset the LINX-10X configuration to factory defaults.</i>
-------------------	---

Important:	<i>Wait at least 30 seconds after power-up of the LINX-10X before pressing the Status Button to ensure that the LINX-10X has booted properly!</i>
-------------------	---

3.6 DIP Switch Settings

The DIP switch assignment for the LINX-10X is shown in Table 2. Please leave all switches at default state.

DIP Switch #	Function	Factory Default
1	Must be OFF	OFF
2	Must be OFF	OFF
3	Must be ON	ON
4	Must be OFF	OFF
5	Must be OFF	OFF
6	Must be OFF	OFF
7	M-Bus enable	OFF

Table 2: DIP Switch Settings for LINX-10X.

3.7 Terminal Layout and Power Supply

The LINX-10X provides screw terminals to connect to the network as well as to the power supply. The screw terminals can be used for wires of a maximum thickness of 1.5 mm²/AWG12. The device can either be DC or AC powered.

Terminal	Function
1	Modbus RS-485 Ground
2	Modbus RS-485 Non-Inverting Input
3	Modbus RS-485 Inverting Input
4	Earth Ground
5, 6	CEA-709 A, B of TP/FT-10 Channel Port
8	Ethernet 100Base-T
15	Earth Ground
16, 17	Power Supply 12 – 35 VDC or 12 – 24 VAC $\pm$ 10 % Do not connect terminal 17 to earth ground!

Table 3: LINX-10X Terminals.

3.8 Wiring

The CEA-709 network segment connected to the LINX-10X needs to be terminated according to the rules found in the specification of the transceiver (see Section 13.1).

Important: *When using shielded network cables, only one side of the cable should be connected to earth ground. Thus, the shield must be connected to earth ground either at the LINX-10X terminals or somewhere else in the network.*

Important: *Never connect terminal 17 to earth ground!*

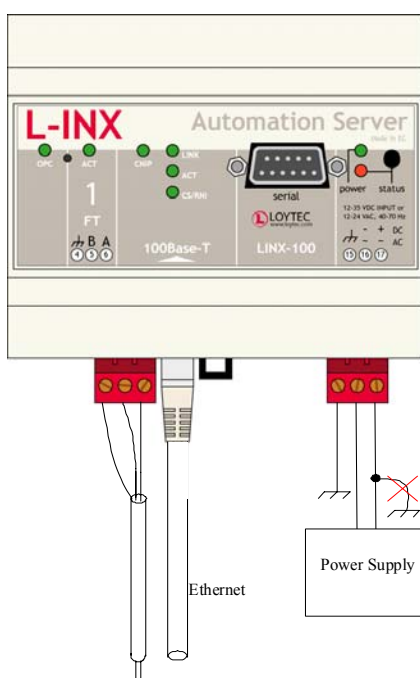


Figure 16: Connecting the LINX-10X.

4 Web Interface

The LINX-10X comes with a built-in Web server and a Web interface to configure the LINX-10X and extract statistics information. The Web interface allows configuring the IP settings, CEA-852 and CEA-709 settings.

4.1 Device Information and Account Management

In a Web browser, enter the default IP address 192.168.1.254 of the LINX-10X. Note that if your PC has an IP address in a subnet other than 192.168.1.xxx, you must open a command tool and enter the following route command to add a route to the LINX-10X.

To Add a Route to the Device

1. Windows **START** → **Run...**
2. Enter 'cmd' and click **OK**.
3. In the command window enter the command line
`route add 192.168.1.254 %COMPUTERNAME%`
4. Then open your Web browser and type in the default IP address '192.168.1.254'.
5. The device information page should appear as shown in Figure 17.

LOYTEC **Device Info**

LINX-100

Device Info

Config

Statistics

L-Web

Reset

Contact

Logout

networks under control

General Info	
Product name	LINX-100
Product code	LINX-100
Firmware	LINX-10x Primary Image
Version	3.5.0
Build date	2010-02-25 16:48:37
Serial number	011501-80000001DFA6
Free memory	8042K, 561K
Free flash	4267K
CPU load	2.6%
System temperature	43.0°C
Supply voltage	23.7V

Project Information	
Project file	linx-21_remote_sched.linx0
Project timestamp	2010-02-18 15:40:13

CEA-709 application unique node IDs and program IDs	
CEA-709	inactive
IP	NID: 80 00 00 01 DF A9 (Online) PID: 90 00 D7 46 16 8A 19 03

Send Service Pin Msg

goahead
WEBSERVER

Figure 17: Device Information Page.

The device information page shows information about the LINX-10X and the current firmware version. It includes the unique node IDs (“Neuron IDs”) of the CEA-709 network interfaces. This page can also be used to send the CEA-709 service pin messages. This is a useful feature when commissioning the LINX-10X, since it is not necessary to be on-site to press the device’s status button.

Click through the menus on the left hand side to become familiar with the different screens. If you click on **Config** in the left menu, you will be asked to enter the administrator password in order to make changes to the settings as shown in Figure 18. Enter the default administrator password ‘admin’ and select **Login**.

LOYTEC **Login**

LINX-100

Device Info

Config

- System
- IP
- Passwords
- Backup/Restore
- CEA-709
- E-mail
- Data Points
- Scheduler
- Calendar
- Alarm

Statistics

networks under control

Enter your username and password

Account:

Password:

Login

Figure 18: Enter ‘admin’ as the default administrator password.

The Config menu opens. Click on **Passwords** in the Config menu, which opens the password configuration page as shown in Figure 19. The LINX-10X has three user accounts: (1) **guest** allows the user to view certain information only, e.g., the device info page. By default the guest user has no password. (2) **operator** is able to read more sensible

information such as calendar data. (3) **admin** has full access to the LINX-10X and can make changes to its configuration. Note that the user accounts are also used to log on to the FTP and Telnet server.

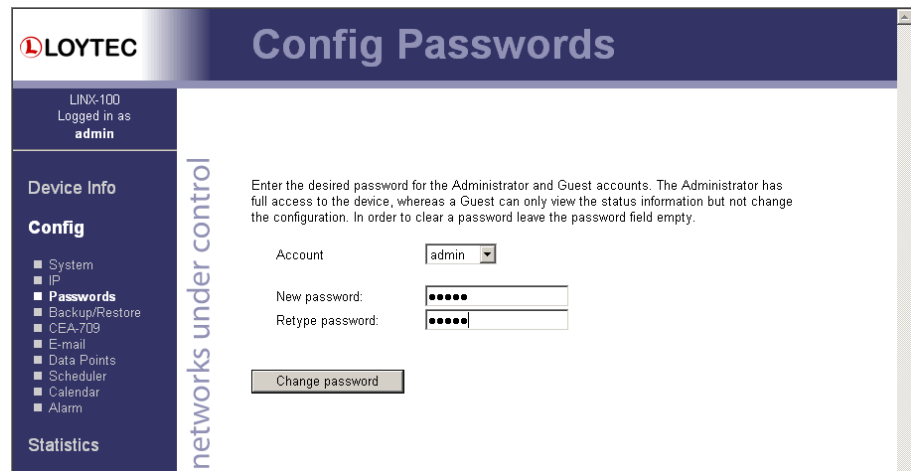


Figure 19: Password Configuration Screen.

Please change the administrator password in order to protect yourself from unwanted configuration changes by anyone else. To do so, select the **admin** account in the drop-down box and enter the new password. If the administrator password is left empty, password protection is turned off and everyone can access the LINX-10X without entering a password. Click on **Change password** to activate the change.

4.2 Device Configuration

The device configuration pages allow viewing and changing the device settings of the LINX-10X. Here are some general rules for setting IP addresses, port numbers, and time values:

- An empty IP address field disables the entry.
- An empty port number field sets the default port number.
- An empty time value field disables the time setting.

4.2.1 System Configuration

The system configuration page is shown in Figure 20. This page allows configuring the device's system time and other system settings. The **TCP/IP Configuration** link is a shortcut to the Ethernet port configuration. Follow that link to change the IP settings of the device.

The time sync source can be set to **auto**, **manual**, **NTP**, or **LonMark**. In the **auto** mode, the device switches to the first external time source that is discovered. Possible external time sources are NTP, LonMark. The option **manual** allows setting the time manually in the fields **Local Time** and **Local Date**. In **manual** mode, the device does not switch to an external time source. Note, that if **NTP** is selected, the NTP servers have to be configured on the IP Configuration page (see Section 4.2.4).

The time zone offset must be defined independently of the time source. It is specified as the offset to GMT in hours and minutes (e.g., Vienna/Austria is +01:00, New York/USA is -06:00). For setting the daylight saving time (DST) predefined choices are offered for Europe and USA/Canada. DST can be switched off completely by choosing **none** or set

manually for other regions. In that case, start and end date of DST must be entered in the fields below.

The screenshot shows the 'Config System' web interface. The top header has the LOYTEC logo and the title 'Config System'. A sidebar on the left contains navigation links: 'Device Info', 'Config', and 'Statistics'. Under 'Config', there are sub-links: 'System', 'Passwords', 'Backup/Restore', 'Port Config', 'CEA-709 Router', 'CEA-852 Server', 'CEA-852 Ch. List', 'E-mail', 'Data Points', 'Trend', 'Scheduler', 'Calendar', and 'Alarm'. The main content area is titled 'networks under control' and contains several configuration sections. The first section is 'Date/Time', with a link to 'Go to TCP/IP Configuration to configure the IP settings.' Below this are fields for 'Time sync source' (set to 'auto'), 'Local Date' (2010-02-26), 'Local Time' (12:14:44), and 'UTC Date/Time' (2010-02-26 11:14:44). There are also fields for 'Timezone offset' (+01:00), 'Daylight saving time (DST)' (Central Europe (CET)), 'DST start' (last Su Mar 02:00), and 'DST end' (last Su Oct 03:00). Buttons for 'Save Date/Time' and 'Get Date/Time' are present. The second section is 'Earth Position', with fields for 'Latitude' (48° 13' 14" N), 'Longitude' (16° 20' 05" E), and 'Altitude' (200 m). Buttons for 'Save Earth Position' and 'Get Earth Position' are also present. The third section is 'CSV Files', with a 'CSV delimiter' dropdown set to a comma. Buttons for 'Save CSV Settings' and 'Get CSV Settings' are at the bottom.

Figure 20: System Configuration Page, e.g., for Vienna, Austria.

The next section on the page allows to configure the LINX-10X's earth position. This setting defines the longitude, latitude and elevation of the device. The latitude and longitude are entered as degrees, minutes, and seconds. The altitude is entered in meters height above sea level. This setting is used for an astronomical clock. For fixed locations such as a building, the position can be entered on this page. For moving locations, this setting can be updated over the network using the network variable nciEarthPos (see Section 12.2.2).

For generating CSV files for trend logs, alarm logs, etc. the delimiter for those CSV files can be configured. This setting can be changes between a comma ',' and a semi-colon ';'. The change takes effect immediately for all files generated by the device.

4.2.2 Backup and Restore

A configuration backup of the LINX-10X device can be downloaded via the Web interface. Press the **Backup/Restore** link as shown in Figure 21 to start the download. The LINX-10X device assembles a single file including all required files. A file requestor dialog allows specifying the location where the backup file shall be stored.

To restore the device settings, simply select a previously generated backup file in the **Restore Configuration** section of the page by clicking the button next to the **Filename** field. Then press the **Restore** button.

The backed up configuration data consists of:

- Device settings (Passwords, IP settings, e-mail config, etc.),
- Data point configuration,

- CEA-709 binding information,
- AST settings,
- L-Web configuration and custom Web pages.

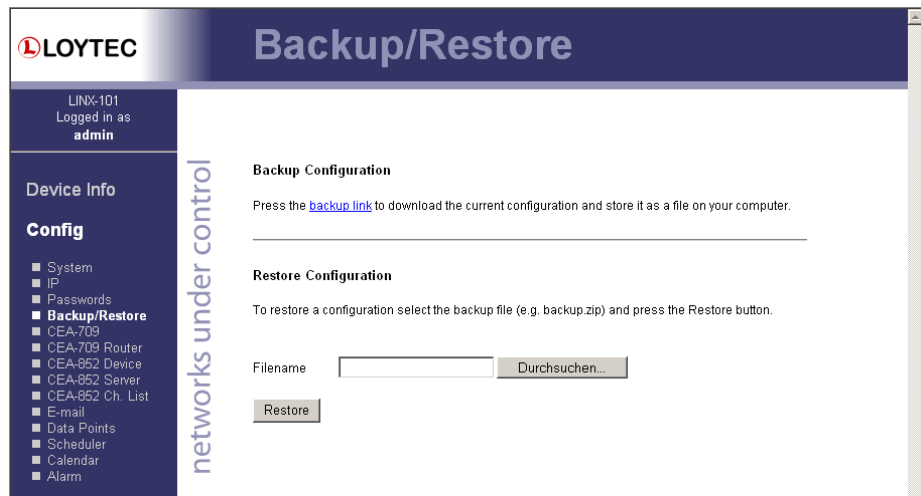


Figure 21: Backup/Restore page.

4.2.3 Port Configuration

This menu allows configuring the device's communications ports. For each communication port, which is available on the device and shown on the label (e.g., Port 1, Port 2, Ethernet), a corresponding configuration tab is provided by the Web UI. An example is shown in Figure 22. Each port tab contains a selection of available communication protocols. By selecting a checkbox or radio button the various protocols can be enabled or disabled on the communication port. Some ports allow exclusive protocol activation only, other ports (e.g., the Ethernet port) allow multiple protocols bound to that port.

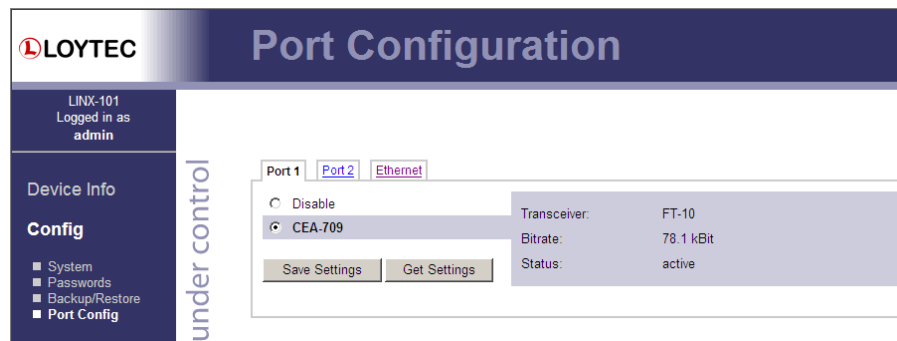


Figure 22: Port Configuration Page.

When selecting a protocol on a communication port, the protocol's communication parameters are displayed in a box on the right-hand side. To save the settings of the currently opened protocol, click the **Save Settings** button. Pressing **Get Settings** retrieves the current settings from the device.

4.2.4 IP Configuration

The TCP/IP configuration is done under the Ethernet port tab as shown in Figure 23. The mandatory IP settings, which are needed to operate the device, are marked with a red asterisk (IP address, netmask, gateway). The **Enable DHCP** checkbox switches between manual entry of the IP address, netmask, and gateway address, and automatic configuration from a DHCP server.

Hostname and **Domainname** are optional entries and can be left empty. For some DHCP configurations it may be necessary to enter a hostname. Please contact your system administrator on how to configure DHCP to acquire an IP address. Further, you can configure up to 3 Domain Name Servers. Currently these entries are not used.

The screenshot shows the LOYTEC Port Configuration web interface. The left sidebar contains a 'Device Info' section and a 'Config' menu with options like System, Passwords, Backup/Restore, Port Config (selected), E-mail, Data Points, Trend, Scheduler, Calendar, and Alarm. The main content area is titled 'Port Configuration' and has tabs for 'Port 1', 'Port 2', and 'Ethernet'. The 'Ethernet' tab is active, showing 'TCP/IP' settings. On the left, there are checkboxes for 'FTP', 'Telnet', and 'HTTP', all of which are checked. Below these are 'Save Settings' and 'Get Settings' buttons. The right side of the form contains various input fields: 'Enable DHCP' (unchecked), 'IP Address' (192.168.24.21), 'IP Netmask' (255.255.192.0), 'IP Gateway' (192.168.1.1), 'Hostname' (empty), 'Domainname' (empty), 'DNS Server 1' through 'DNS Server 3' (all empty), 'MAC Address' (00:0A:B0:01:0C:9F) with a 'Use Factory Default' checkbox checked, 'NTP Server 1' (10.101.17.2), 'NTP Server 2' (empty), 'NTP Status' (in-sync), and 'Link Speed & Duplex' (Auto Detect). A note at the bottom states: 'The entries marked with (*) are required for proper operation'.

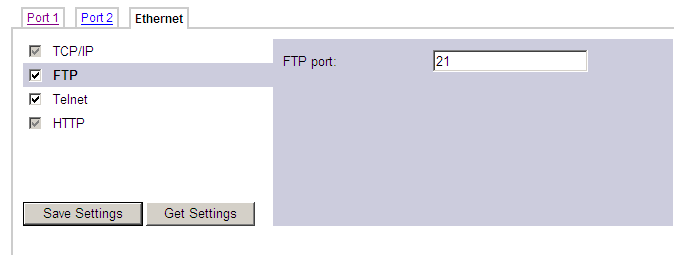
Figure 23: IP Configuration Page.

The device comes configured with a unique MAC address. This address can be changed in order to clone the MAC address of another device. Please contact your system administrator to avoid MAC address conflicts.

The device can be configured to synchronize its clock with NTP time. Enter the IP address of a primary and, optionally, a secondary NTP server. The LINX-10X will use NTP as a time source if the time sync source in the system configuration page is set to **NTP** (see Section 4.2.1). The field **NTP status** below the NTP server settings displays the current NTP synchronization status (**out-of-sync**, or **in-sync**).

If the device is operated with a 10 Mbit/s-only hub, the link speed should be switched from **Auto Detect** to **10Mbps/Half-Duplex**. With modern 100/10 Mbit/s switches, this setting can be left at its default.

Other standard protocols that are bound to the Ethernet interface are FTP, Telnet, and HTTP (Web server). By deselecting the checkbox, those protocols can be individually disabled. The standard UDP/TCP ports can be changed in the respective protocol settings. An example for the FTP server is shown for FTP in Figure 24. The FTP server is used for instance to update the firmware (see Section 14.1) or to upload a new data point configuration. Note that HTTP for the Web server can only be disabled on the console interface or by using the device configuration of the Configurator.

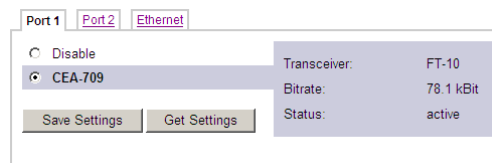


The screenshot shows the 'Ethernet' tab selected. On the left, there are four checked checkboxes: TCP/IP, FTP, Telnet, and HTTP. Below these are 'Save Settings' and 'Get Settings' buttons. On the right, there is a label 'FTP port:' followed by a text input field containing the number '21'.

Figure 24: FTP server configuration on the Ethernet port.

4.2.5 CEA-709 Configuration

The CEA-709 protocol can be enabled on the device's ports Port1, Port2, etc. if available. To enable it, click the **CEA-709** radio button as shown in Figure 25. Note, that depending on the device model, other protocols on the same port will be disabled in this case. The protocol settings box on the right-hand side displays the current transceiver settings.



The screenshot shows the 'Ethernet' tab selected. On the left, there are two radio buttons: 'Disable' and 'CEA-709'. The 'CEA-709' radio button is selected. Below these are 'Save Settings' and 'Get Settings' buttons. On the right, there is a settings box with three rows: 'Transceiver:' with the value 'FT-10', 'Bitrate:' with the value '78.1 kBit', and 'Status:' with the value 'active'.

Figure 25: CEA-709 Configuration Page.

4.2.6 CEA-852 Device Configuration

The CEA-852 protocol is only available on the Ethernet port. To enable CEA-852 on the device, select the **CEA-852 (CEA-709 over IP)** checkbox on the **Ethernet** tab of the port configuration page. Please note that on device models without a router or a proxy, the CEA-709 protocol on other ports will be disabled (e.g., LINX-100).

The CEA-852 protocol settings are displayed in the settings box on the right-hand side as shown in Figure 26. Typically, the device is added to an IP channel by entering the relevant information on a configuration server. The configuration server then contacts the CEA-852 device of the LINX-10X and sends its configuration.

Figure 26: CEA-852 Device Configuration Page.

The field **Config server address** and **Config server port** display the IP address and port of the configuration server, which manages the LINX-10X and the IP channel. The field **Config client port** represents the IP port of the LINX-10X's CEA-852 device. This setting should be left at its default (1628) unless there are more than one CEA-852 devices operating behind a single NAT router. Please refer to the L-IP User Manual [1] to learn more about NAT configuration.

In the field **Device name** the user can enter a descriptive name for the LINX-10X, which will appear in the IP channel to identify this device. You can enter a device name with up to 15 characters. It is recommended to use unique device names throughout the IP channel.

The **Channel mode** field reflects the current channel mode of the CEA-852 device. It is configured by the configuration server. If there are any two devices in the channel which use the same IP address but different ports (e.g., multiple LINX-10X behind one NAT router) the channel switches to **Extended NAT mode**. Please refer to the L-IP User Manual [1] to learn more about configuring the Extended NAT mode in the configuration server.

The configuration server sets the **SNTP server** addresses and the **Channel timeout**.

The field **Escrow timeout** defines how long the CEA-852 device on the LINX-10X waits for out-of-sequence CEA-852 data packets before they are discarded. Please enter the time in ms or '0' to disable escrowing. The maximum time is 255 ms.

The field **Aggregation timeout** defines the time interval in which multiple CEA-709 packets are combined into a single CEA-852 data packet. Please enter the time in ms or '0' to disable aggregation. The maximum time is 255 ms. Note that disabling aggregation will negatively affect the performance of the CEA-852 device of the LINX-10X.

The field **MD5 authentication** enables or disables MD5 authentication. Note that MD5 authentication cannot be used together with the Echelon's *i.LON 1000* since the *i.LON 1000* is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i.LON 600*. In the following field **MD5 secret** enter the 16-byte MD5 secret. Note that for security purposes the active MD5 secret is not displayed. You may enter the 16 bytes as one string or with spaces between each byte, e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

Also note that entering the MD5 secret on the Web interface may pose a security risk. Since the information is transmitted over the network it can be subject for eavesdroppers on the line. It is recommended to use a cross-over cable.

In the field **Location string** the user can enter a descriptive text which identifies the physical location of the LINX-10X. A location string can have a maximum length of 255 characters. This is optional and for informational purposes only.

If the CEA-852 device on the LINX-10X is used behind a NAT router, the public IP address of the NAT router or firewall must be known. To automatically detect the NAT address leave the **Auto-NAT** checkmark enabled.

The **Multicast Address** field allows the user to add the CEA-852 device of the LINX-10X into a multi-cast group for the CEA-852 IP channel. Enter the channel's IP multi-cast address here. Please contact your system administrator on how to obtain a valid multi-cast address. To learn when it is beneficial to use multi-cast addresses in your channel please refer to the L-IP User Manual [1].

4.2.7 CEA-709 Router Configuration

This page is only available on the LINX-101. The CEA-709 router configuration page allows configuring the built-in router mode. Available modes are **Configured Router** and **Smart Switch**. The LINX-101 must be rebooted to let the changes on this page take effect.

The configured router mode is the default setting. Choose this setting if you want to use the LINX-101 as a standard configured CEA-709 router that can be configured in a network management tool such as NL-200 or LonMaker.

The Smart Switch mode lets the device act as a self-learning router like the L-Switch. In this configuration the LINX-101's router doesn't need to be configured with a network management tool but is completely transparent in the network. Use this operating mode in a plug&play networking environment. The switch mode should only be used in LAN networks. In Smart Switch mode, this page has two more configuration fields: **Subnet/node learning** and **Group learning**.

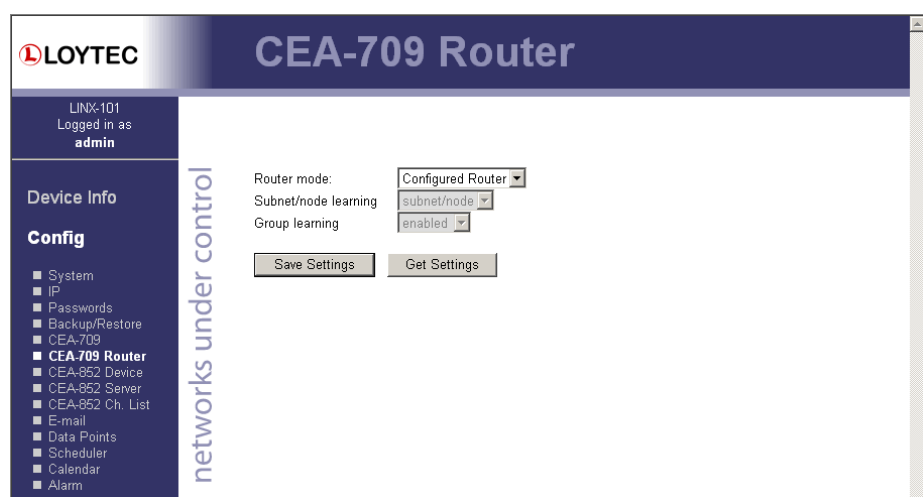


Figure 27: CEA-709 Router Configuration Page.

4.2.8 CEA-852 Server Configuration

This page is only available on the LINX-101. On this configuration page the configuration server on the LINX-101 can be enabled or disabled. In the drop-down box **Config server status** select **enabled** and click on **Save Settings** to activate the configuration server. Then the configuration server settings page appears as shown in Figure 28. If the configuration

server is enabled the green configuration server LED labeled **CS** will be on, otherwise it will be off.

The configuration server port can be changed in the **Config server port** field. It is recommended to keep the default port setting of 1629. The field **Channel name** is informational only and can consist of up to 15 characters.

The field **Channel members** displays the current number of members on the IP-852 channel. The field **Channel mode** reflects the current channel mode. The LINX-101 configuration server automatically determines this mode. Depending on if there are any two devices in the channel which use the same IP address but different ports (e.g., multiple CEA-852 devices behind one NAT router). If all IP addresses are unique, the mode is **Standard**, if some are not unique the mode is **Extended NAT mode**. Please refer to Section 7.4.2 to learn more about the implications of this mode.

Figure 28: Configuration server settings.

Enter NTP timer server address and ports in the fields **Primary SNTP** and **Secondary SNTP**. The LINX-101 will synchronize to NTP time if primary or primary and secondary NTP servers are specified. A list of available timeservers can be found at www.ntp.org.

The **Channel timeout** is an IP-852 channel property and indicates how old a packet can be before it is discarded. The channel timeout is set in ms. To disable the channel timeout enter a value of 0. To select the proper value please consult Section 7.7.1. Setting a channel timeout other than 0 requires a valid SNTP server entry on the configuration server.

The **Auto members** option allows members to be automatically added to the channel. If turned on, CEA-852 devices can register on the IP-852 channel without the device being explicitly added on the configuration server. This special feature is useful in combination with the LPA-IP since it can add itself to the configuration server during the debug session. Non-responding auto members are automatically removed from the channel. This feature is turned off by default and must be explicitly turned on. Use this option with care because new CEA-852 devices can add themselves to the channel without knowledge of the system operator. This could cause a potential security hole.

The **Roaming members** option allows tracking CEA-852 devices when their IP address changes. This feature must be turned on if DHCP is used and the DHCP server can assign different IP addresses to the same device (same Neuron-ID). In combination with Auto-NAT the LINX-101's router can also be operated behind NAT routers, which change their IP address between connection setups. For more information on this topic refer to Section 7.4.1. The roaming member feature is turned on by default. It is recommended to turn off this feature if DHCP is not used or if the DHCP server always assigns the same IP address to a given MAC address.

Use the drop-down box **MD5 authentication** to enable and disable MD5 authentication. If MD5 authentication is enabled, all devices on the IP-852 channel must have MD5 enabled and must use the same MD5 secret. Note that MD5 authentication cannot be used together with the Echelon's *i.LON* 1000 since the *i.LON* 1000 is not fully compliant with the CEA-852 authentication method. MD5 can be used with the *i.LON* 600. The MD5 secret can be entered over the Web interface. You may enter the 16 bytes as one string or with spaces between each byte,

e.g., 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF.

It is recommended, however, to enter the secret locally and not over an Internet connection. It is best to use a cross-over Ethernet cable connected to the PC.

4.2.9 CEA-852 Channel List

This page is only available on the LINX-101. If the configuration server is enabled on the LINX-101, the CEA-852 device list can be seen in the CEA-852 channel list menu. An example is given in Figure 25.

The **Add Device** button is used to add another CEA-852 device to the IP-852 channel. The **Reload** button updates the Web page and the **Recontact** button contacts all devices to update their status. The **Execute** button executes the option selected in the adjacent drop-down box on the checked members. Each member can be selected for that action in an individual check-box in the **Sel** column. Actions available are: **disable**, **enable**, **delete**, **assign to NAT**, and **remove from NAT**. For more information on the actions on NAT routers refer to Section 7.4.2.

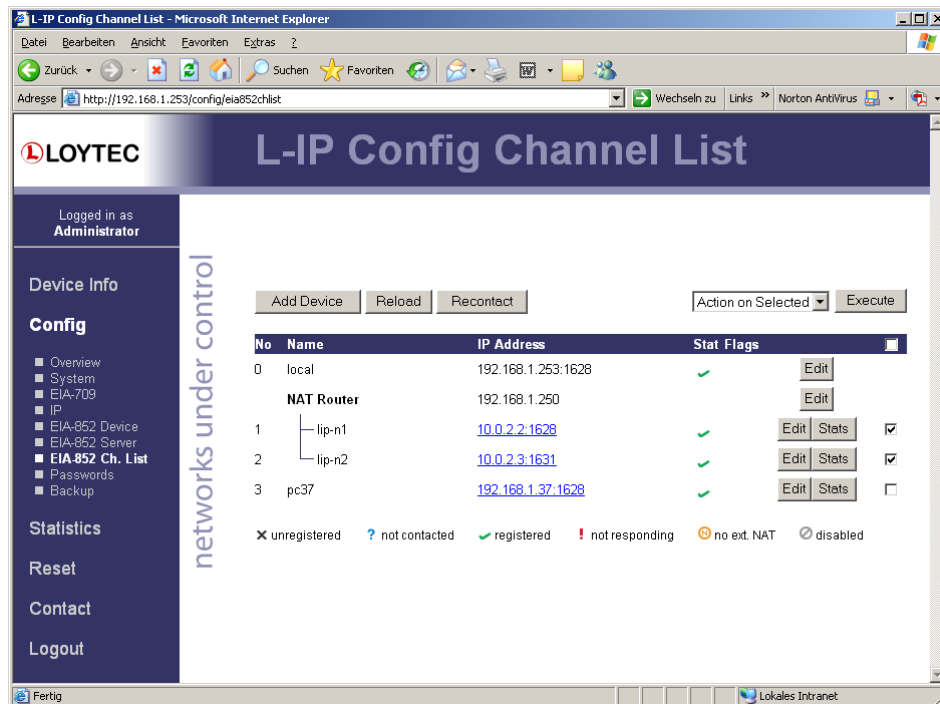


Figure 29: CEA-852 channel membership list.

The device status information is indicated with descriptive icons of different colors. The description for the different status indicators is shown in Table 4. The **Flags** column indicates with an **A** that the device is an auto member.

Click on the **Edit** button to change the device name, IP address, and port number for this device. Click **Edit** on a NAT router to change the NAT router address. The **Stats** button retrieves the statistics summary page from the client device.

Icon	Status	Description
	registered	The CEA-852 device has been successfully registered with the IP-852 channel and is fully functional.
	unregistered	The CEA-852 device has never been registered with the IP-852 channel.
	not contacted	The CEA-852 device has not been contacted since the configuration server has started.
	not responding	The CEA-852 device has been registered but is not responding at the moment.
	disabled	The CEA-852 device has been disabled on the channel (or rejected).
	No extended NAT	The CEA-852 device does not support the extended NAT mode. This device is disabled.

Table 4: Possible Communication Problems in the Configuration Server.

4.2.10 E-mail Configuration

The Web interface provides the e-mail configuration page to set up an e-mail account, which is used to send e-mails. The content and time when e-mails are sent is configured through the Configurator software (see Section 6.9). The e-mail configuration page is shown in **Fehler! Verweisquelle konnte nicht gefunden werden.**

In the field for the outgoing e-mail server, enter the SMTP server of your Internet provider. Typically, the SMTP server port can be left at 25. In the field **Source E-mail Address**, enter the e-mail address of the LINX-10X's e-mail account. In the field **Source E-mail Sender Name** enter a name that the e-mail will display as the source name. Note, that only ASCII characters are allowed in the name. If replies shall be sent to another e-mail address, specify this in the **Reply E-mail Address**.

If the provider's SMTP server requires authentication, enter the required user name and password. Note, that only username/password is supported. SSL/TLS authentication is not supported by the LINX-10X (e.g., Hotmail, gmail cannot be used).

To verify the e-mail configuration, reboot the device to let the changes take effect and return to the e-mail configuration page. Then press one of the **Send Test E-mail** buttons. Note, that a DNS server must be configured in the IP settings (see Section 4.2.4) to resolve the e-mail server host name. The Web UI displays a warning message at the top of the page, if the DNS configuration is missing.

Figure 30: E-mail Configuration Page.

4.2.11 Data Points

The device's Web interface provides a data point page, which lists all configured data points on the device. An example is shown in Figure 31. The data point page contains a tree view. Clicking on a particular tree item fills the right part of the page with a data point list of that tree level and all levels below. Thus, one can get an easy overview of all data points.

The data point list displays the data point name, direction, type, current value, and data point state. Inactive points are displayed in gray. If the data point list does not fit on one page, there are page enumerator links at the bottom. Important data point states and their implications are listed in Table 5.

LOYTEC Data Points

LINX-101
Logged in as
admin

Device Info

Config

- System
- Passwords
- Backup/Restore
- Port Config
- CEA-709 Router
- CEA-852 Server
- CEA-852 Ch. List
- E-mail
- Data Points**
- Trend
- Scheduler
- Calendar
- Alarm

Statistics

networks under control

ROOT

- System Registers
- User Registers
- CEA709 Port
- CEA852 Port

Reload

Folder: /System Registers/

Name	Dir.	Type	Value	State
System Time	input	analog	1267190525	normal
CPU Load	input	analog	7.8	normal
Free Memory	input	analog	8415116	normal
Free Flash	input	analog	3871588	normal
Supply Voltage	input	analog	15.1	normal
System Temp	input	analog	41.5	normal
Application Vendor	input	analog	--	invalid value
Authentication Code	output	analog	--	invalid value
Authentication Result	input	binary	FALSE	normal
Serial Number	input	string	011301-800000039E88	normal
MAC Address	input	user	000AB00126F7	normal
Firmware Version	input	string	3.5.0	normal
Device IP Address	input	string	192.168.24.101	normal
Device IP Port	input	analog	80	normal
TZ Offset	input	analog	3600	normal

Figure 31: Data point page.

Data Point Status	Description
normal	The data point is in normal operation state and possesses a value.
invalid value	The data point has no valid value.
offline (config)	The data point has a value but it is not reflected on the network due to a configuration error (not commissioned, no binding, no client mapping, etc.)
offline	The data point has a value but it is not reflected on the network due to a communication error (e.g., the peer node is not online).
unreliable (offline)	The data point has a value but it is considered unreliable because it was derived from a source, which was offline (e.g., the value was fed from a connection, where the source is offline).
unreliable (range)	The data point has a value but it is considered unreliable because the value source specified an out-of-range value. The value is limited to the supported range.
unreliable	The data point has a value but it is considered unreliable for an unspecified reason.
not configured	The data point is mapped to a port, which is not configured (e.g., the port is disabled).
Line grayed-out	The data point is inactive. Values can be written but no network communication is triggered. This can be the case, if a data point is not used in the configuration or it is connected to a dynamic NV, which is not present on the device.

Table 5: Data Point States.

The data point names are links. Clicking on such a link opens a detailed page on that data point. If the data point supports it, the user can also enter a new data point value as depicted in Figure 32. The **Status** field is discussed in Table 5. The **Flags**, **Poll cycle**, **Min/Max send time** and **Max age** fields are the common timing parameters for the data point. See Section 5.2.2 for a closer discussion on timing parameters.

Data Point Details

networks under control

[back](#)
Reload

Data Point Details	
Path	/CEA709 Port/Datapoints/tn50/
Name	NV_tn50Controller_1nvo00temp
Direction	input
Type	analog
Value	20 degrees Celsius Set
Timestamp	26.02.2010 13:24:21
Status	normal
Flags	
Poll cycle	0 ms
Min. send time	0 ms
Max. send time	0 ms
Max age	-1 ms
Description	
Native Name	

Figure 32: Data point details page.

Clicking on the **Set** button writes the new value to the device's data server. When setting a value, the Web page displays the status of the action:

- **Successfully set value:** The new value has been successfully set in the data point and the update has been sent on the network, if it is a network data point.
- **Could not send value update:** The new value has been set but it has not been sent out on the network. The reason can be that the peer node is currently offline or there is a configuration error. The data point status reflects this error.
- **Could not set value (error code):** The new value has not been set because of an internal error. Please contact LOYTEC with the error code.

4.2.12 Trend

The Web interface provides a configuration page to re-configure trend logs at run-time. The changes made to the trend logs take effect immediately without the needs for a reboot of the device. Allocating new trend logs can only be done in the configuration software (see Section 6.13.1). The trend log main page displays all available trend logs. Click on the trend log to be edited. This opens the trend log configuration page. An example is shown in Figure 33.

Figure 33: Trend log configuration page.

The user can change the **Trend Mode**, the **Fill Mode**, the **Log Interval** and the **Fill Level Notification**. Furthermore, data points can be added to the trend log by clicking the **Add...** button. A data point selector dialog opens. Click on a data point for adding it. For removing a data point from the trend log, click on it in the **Logged Data Points** list and hit the **Remove** button. Save the changes made by clicking the **Save** button. For more information on how a trend log can be configured please refer to the Configurator Section 6.13.

4.2.13 Scheduler

The Web interface provides the scheduler page to edit its schedules at run-time, i.e., change the times and values that shall be scheduled. Allocating new schedules can only be done in the configuration software (see Section 6.11). The scheduler main page displays all available schedules. Click on the schedule to be edited. This opens the scheduler page. An example is shown in Figure 34.

The **effective period** defines when this schedule shall be in effect. Leave **From** and **To** at ‘*.*.*’ to make this schedule always in-effect. Otherwise enter dates, such as ‘30.1.2000’. To entirely disable a scheduler de-select the **Enable Schedule** check box.

Schedules are defined per day. On the left-hand side, the weekdays **Monday** through **Sunday** can be selected, or exception days from the calendar, e.g., Holidays. Once a day is selected, the times and values can be defined in the daily planner on the right-hand side. In the example shown in Figure 34, on Monday the value **day** is scheduled at **8:00am**. The same principle applies to **exception days**. **Exception days** override the settings of the normal weekday. Put a check mark on those exception days from the calendar, which shall be used in the schedule. To edit the date ranges of exception days click on the links to the used calendars, e.g., ‘calendar’ or ‘Scheduler_1’. The ‘Scheduler_1’ is a calendar, which is embedded into the schedule and not accessible by other schedulers. For more information on how to set up schedules and calendars refer to Section 6.11.

To define actual values for the names such as **day** click on the tab **Presets** as shown in Figure 35. Which data points are scheduled is determined by the configuration software. On this page, only the actual values can be changed. To define a new value, click on the button **Add Preset**. This adds a new column. Enter a new preset name (e.g., ‘day’). Then

enter values for the data points in the **preset** column. The **data point name** column displays the short-hand name defined in the configuration software.

Figure 34: Schedule Configuration Page.

Figure 35: Scheduled Presets Configuration Page.

You can switch back and forth between the two tabs. Once the configuration is complete, click on the **Save** button. This updates the schedule in the device. Any changes made become effective immediately.

On local schedulers the Web UI also allows to reconfigure the scheduled data points. This change takes effect immediately without a reboot of the device. To add and remove data points to the scheduler, go to the **Data Points** tab. The configuration page is depicted in Figure 36. To add a new data point, click the **Add...** button. To remove a data point, select the the data point in the list **Scheduled Data Points** by clicking on it and then press the **Remove** button. Finally, store the changes by clicking the **Save** button. After modifying the scheduled data points, go back to the Presets tab and enter descriptive value label names. For more information on how to configure a scheduler please refer to the Configurator Section 6.11.4.

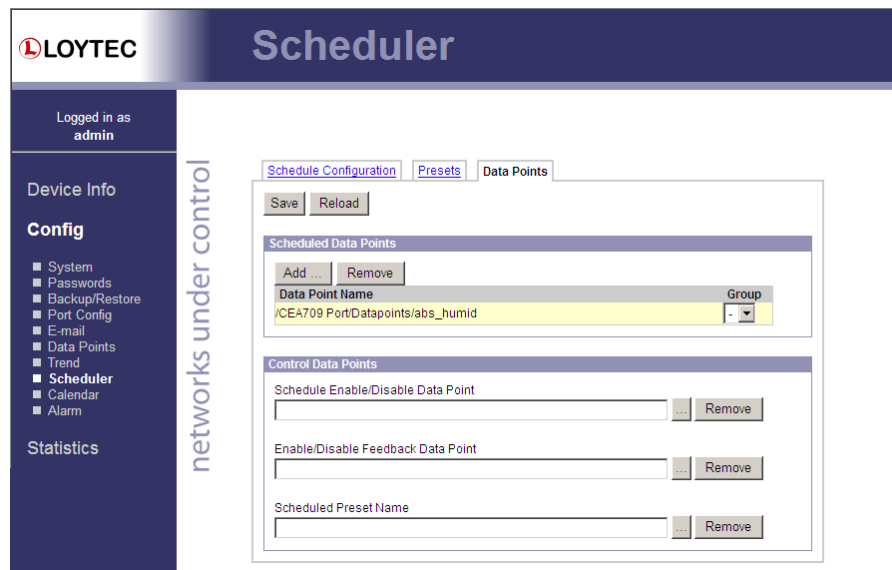


Figure 36: Re-configure scheduled data points on the Web UI.

4.2.14 Calendar

The Web interface provides the calendar page to edit its calendars at run-time, i.e. change the exception days. The calendar main page displays all available calendars. Click on the calendar to be edited. This opens the calendar configuration page. An example is shown in Figure 37.

The **effective period** defines when this calendar shall be in effect. Leave **From** and **To** at ‘*.*.*’ to make this calendar always in-effect. Otherwise enter dates, such as ‘30.1.2000’.

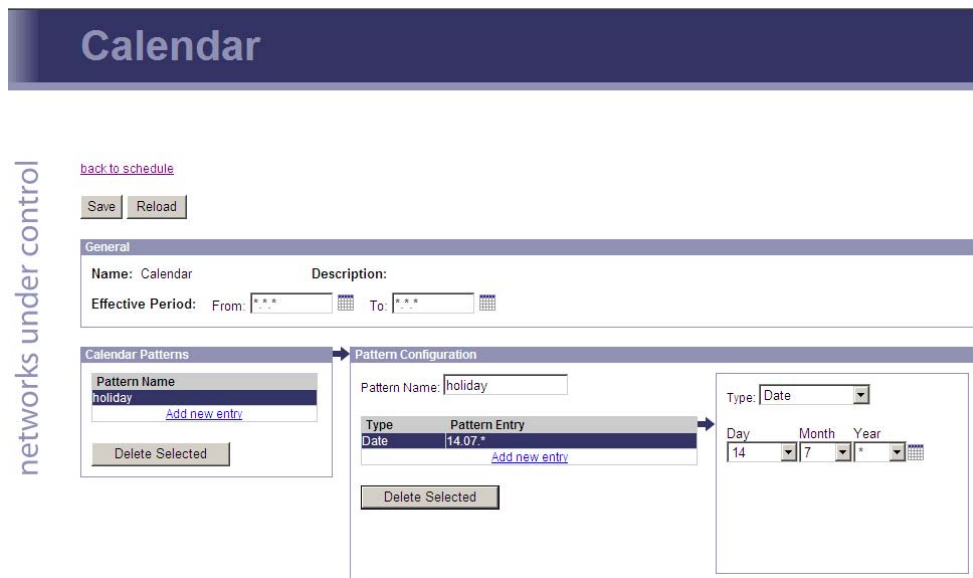


Figure 37: Calendar Configuration Page.

On the remainder of this page, work from left to right. Click on a calendar pattern or create a new calendar pattern by clicking **Add new entry**. A calendar pattern defines a set of pattern entries, which defines the actual dates or date ranges. In the example in Figure 37, the calendar pattern **Holidays** is selected.

In the **Pattern Configuration** box, the calendar pattern’s name can be edited. It also lists the entries. New entries can be added by clicking **Add new entry**. Existing entries can be

selected and edited in the box on the right-hand side. In the example in Figure 37, the date **14.7.*** is selected, which means “The 14.7. of every year”. Other entry types such as **Date Range** and **Week-and-Day** can be selected. See Section 5.4.3 for more information about defining exception dates.

4.2.15 Alarm

The Web interface provides the alarm page to view the currently pending alarms of its alarm data points. The alarm main page displays all available alarm data points. Alarm objects which have active alarms are displayed in red. Click on the alarm object to be viewed. This opens the alarm summary page. An example is shown in Figure 38.

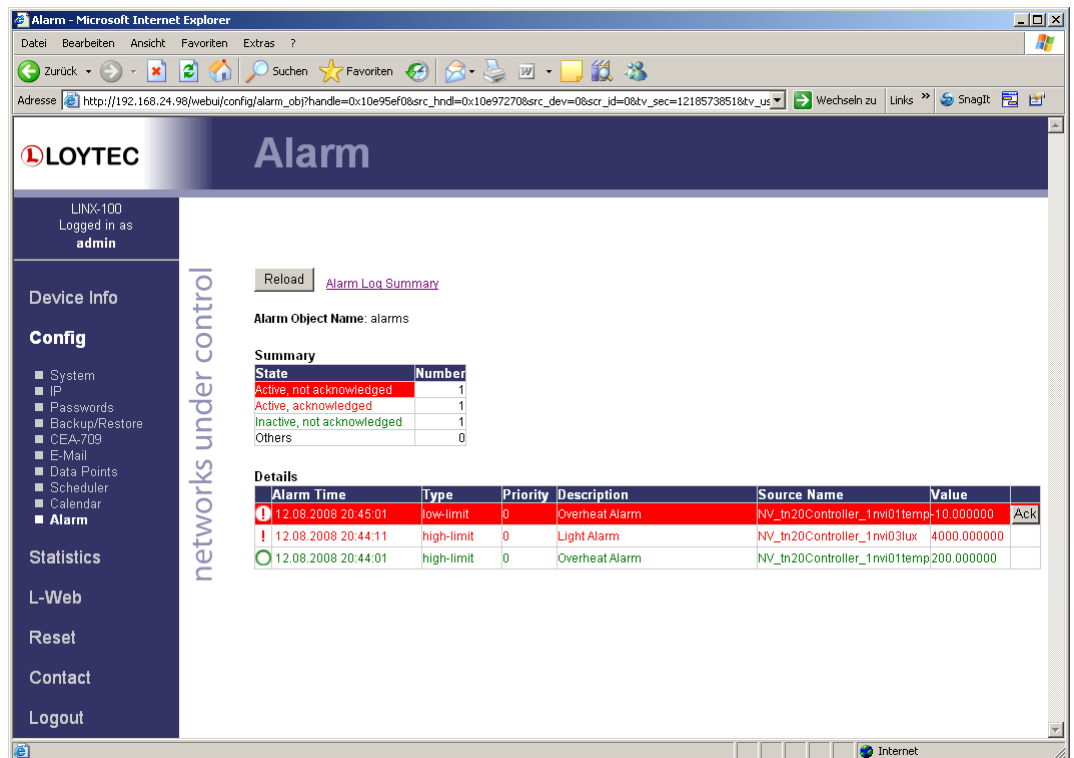


Figure 38: Alarm Summary Page.

Active alarms are highlighted red. Inactive alarms which have not been acknowledged are rendered in green. Alarms that can be acknowledged have an **Ack** button. Press on the **Ack** button to acknowledge the alarm. Depending on the technology, this and older alarm records will be acknowledged. Acknowledged, active alarms are rendered in red. Click on **Reload** to refresh your alarm list.

Inactive alarms that have been acknowledged disappear from the list. To record historical information about those alarms, the alarm log must be used. See Section 4.3.8 for the alarm log Web interface.

4.3 Device Statistics

The device statistics pages provide advanced statistics information about the CEA-709 device, the CEA-852 device, the System Log, the scheduler, the Alarm Log and the Ethernet interface.

4.3.1 IP Statistics

Figure 39 shows the IP statistics page. It allows finding possible problems related to the IP communication. Specifically, any detected IP address conflicts are displayed (if the LINX-10X's IP address conflicts with a different host on the network).

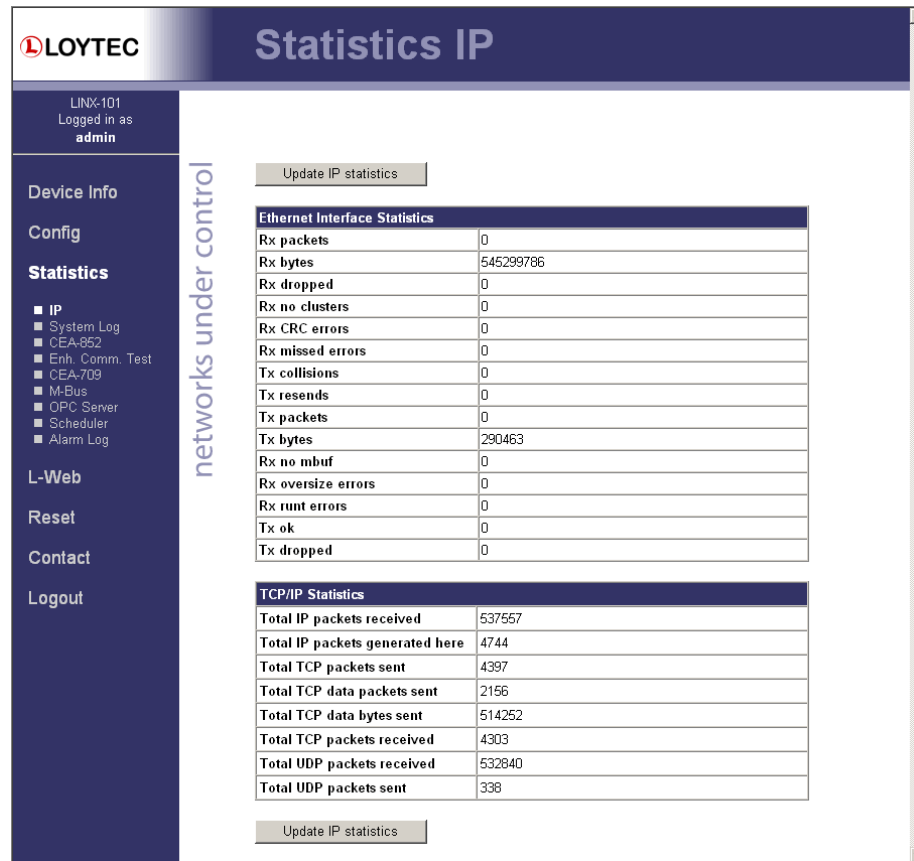


Figure 39: IP Statistics Page.

4.3.2 CEA-852 Statistics

The CEA-852 statistics page displays the statistics data of the CEA-852 device on the LINX-10X. It is only displayed if the CEA-852 interface is enabled. The upper part of the CEA-852 statistics page is depicted in Figure 40. To update the statistics data, press the button **Update all CEA-852 statistics**. To reset all statistics counters to zero, click on the button **Clear all CEA-852 statistics**. The field **Date/Time of clear** will reflect the time of the last counter reset.

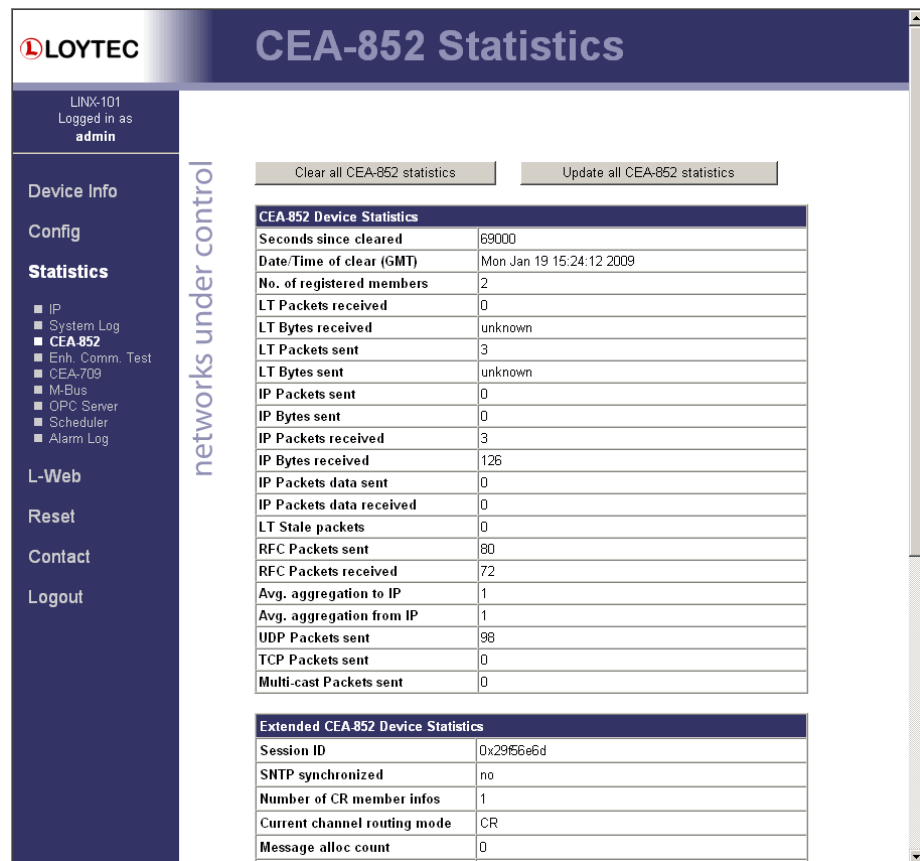


Figure 40: Part of the CEA-852 Statistics Page.

4.3.3 Enhanced Communications Test

The Enhanced Communications Test allows testing the CEA-852 communication path between the CEA-852 device on the LINX-10X and other CEA-852 devices as well as the configuration server. The test thoroughly diagnoses the paths between individual members of the IP channel and the configuration server in each direction. Port-forwarding problems are recognized. For older devices or devices by other manufacturers, which do not support the enhanced test features, the test passes as soon as a device is reachable, but adds a comment, that the return path could not be tested. A typical output is shown in Figure 41.

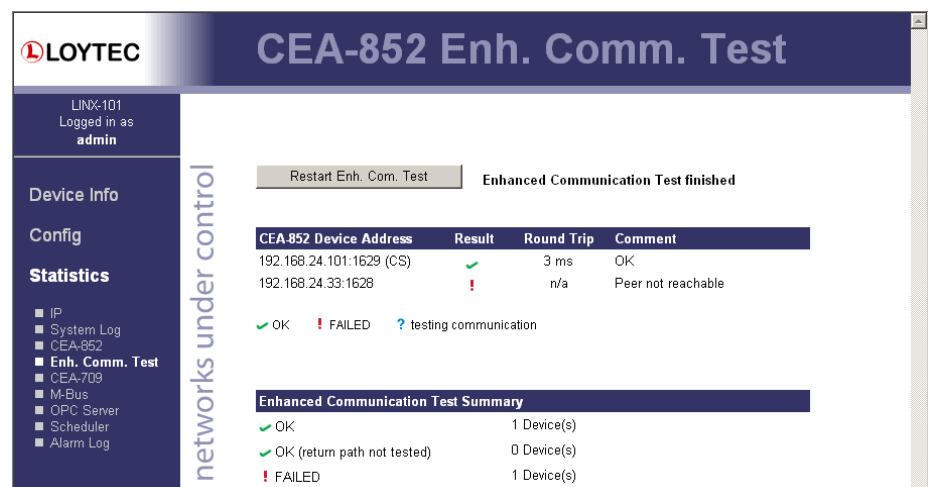


Figure 41: Enhanced Communication Test Output.

The Round Trip Time (RTT) is measured as the time a packet sent to the peer device needs to be routed back to the LINX-10X. It is a measure for general network delay. If the test to a specific member fails, a text is displayed to describe the possible source of the problem. The reasons for failure are summarized in Table 6.

Text displayed (Web icon)	Meaning
OK, Return path not tested (green checkmark)	Displayed for a device which is reachable but which does not support the feature to test the return path (device sending to this CEA-852 device). Therefore a potential NAT router configuration error cannot be detected. If the tested device is an L-IP, it is recommended to upgrade this L-IP to 3.0 or higher.
Not reachable/not supported (red exclamation)	This is displayed for the CS if it is not reachable or the CS does not support this test. To remove this uncertainty it is recommended to upgrade the L-IP to 3.0 or higher.
Local NAT config. Error (red exclamation)	This is displayed if the CEA-852 device of the LINX-10X is located behind a NAT router or firewall, and the port-forwarding in the NAT-Router (usually 1628) or the filter table of the firewall is incorrect.
Peer not reachable (red exclamation)	Displayed for a device, if it is not reachable. No RTT is displayed. The device is either not online, not connected to the network, has no IP address, or is not reachable behind its NAT router. Execute this test on the suspicious device to determine any NAT configuration problem.

Table 6: Possible Communication Problems.

4.3.4 CEA-709 Statistics

The CEA-709 statistics page displays statistics data of the CEA-709 port on the LINX-10X as shown in Figure 42. This data can be used to troubleshoot networking problems. To update the data, click on the button **Update CEA-709 statistics**.

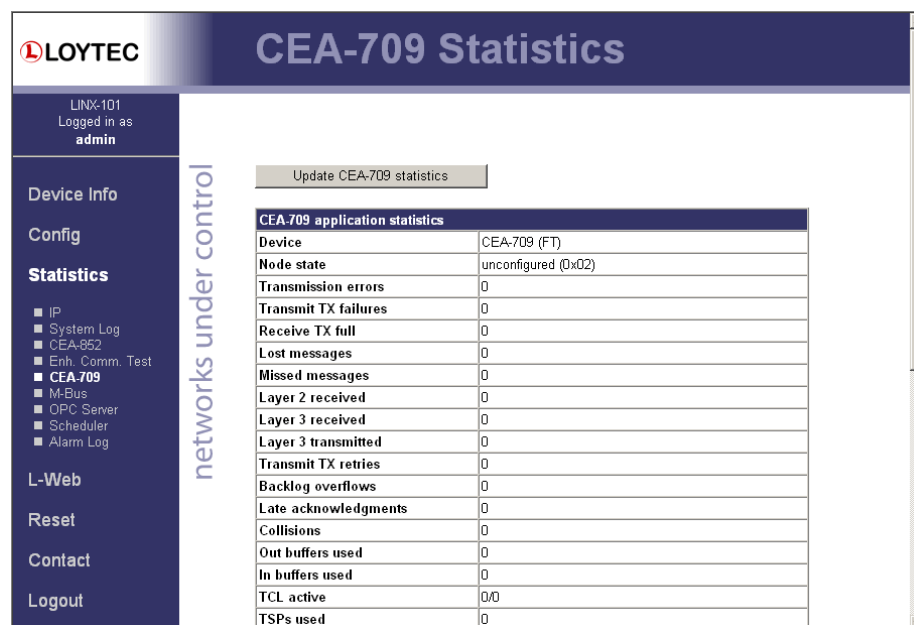


Figure 42: CEA-709 Statistics Page.

4.3.5 System Log

The System Log page prints all messages stored in the system log of the LINX-10X. An example is shown in Figure 43. This log data is important for trouble-shooting. It contains

log entries for reboots and abnormal operating conditions. When contacting LOYTEC support, have a copy of this log ready.

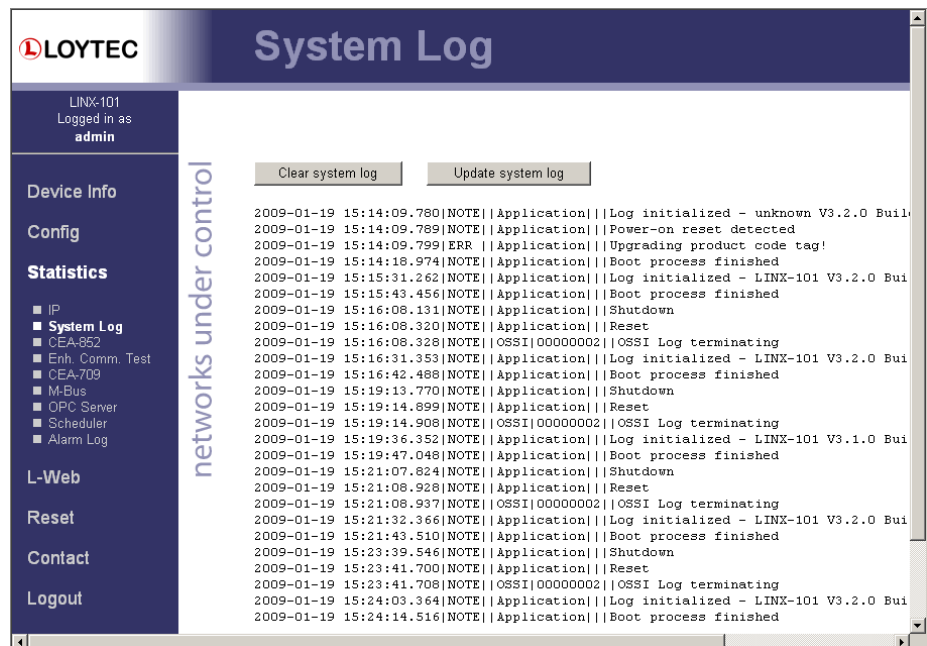


Figure 43: System Log Page.

4.3.6 OPC Server Statistics Page

The OPC server statistics page shows statistics data, which contains information on currently and previously connected clients. An example list of OPC clients is shown in Figure 44. Clicking on the **Update OPC statistics** button retrieves the current statistics.

The **Summary** table on the top of the page displays the number of currently connected clients. These clients occupy TCP connections. The next line specifies the total number of accepted client connections since the device is running. The figure for rejected connections can be used to detect situations, where too many clients try connecting at the same time.

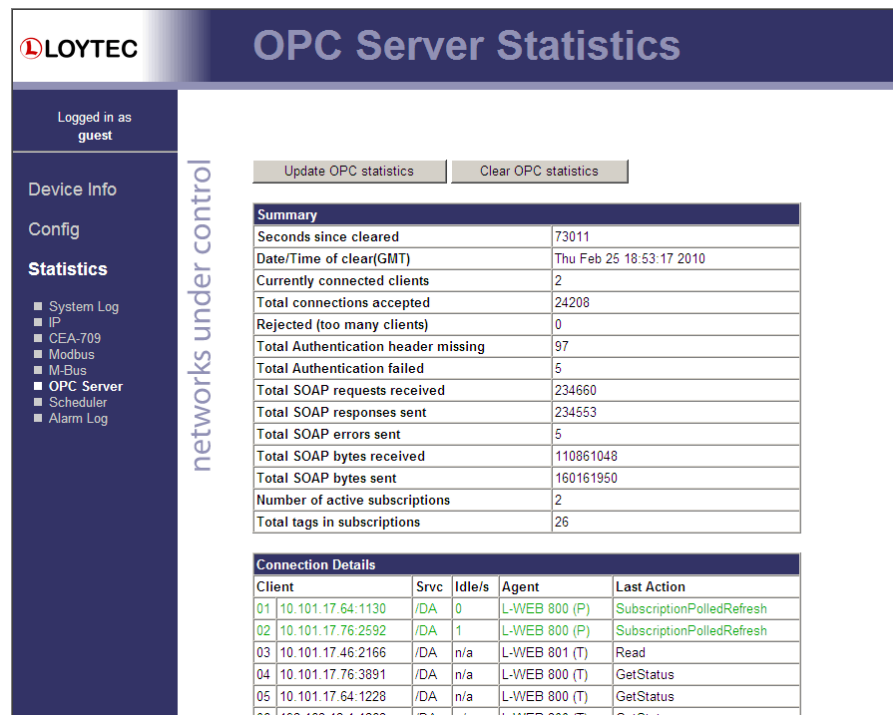


Figure 44: OPC Server Statistics Page.

The **Connection Details** list shows more information on the history of client connections. The green lines at the top denote currently active connections. Active connections have an idle time figure specified in seconds. The following lines in black represent a history of the most recent connections. Inactive connections read “n/a” in the **Idle** column.

All lines contain client information, which specifies the client IP address and port of the connected client. The **Srvc** column specifies the type of Web service (Web, DA, DL). The **Agent** column contains information on the HTTP agent of the client, and the **Last Action** column contains information on the last known Web service SOAP action the client has requested.

4.3.7 Scheduler Statistics Page

The scheduler statistics page provides an overview of what is scheduled at which day and which time. In the **Display Schedules** list, select a single schedule to view its scheduled values and times. Use the multi-select feature to get the overview of more schedules. An example is shown in Figure 45.

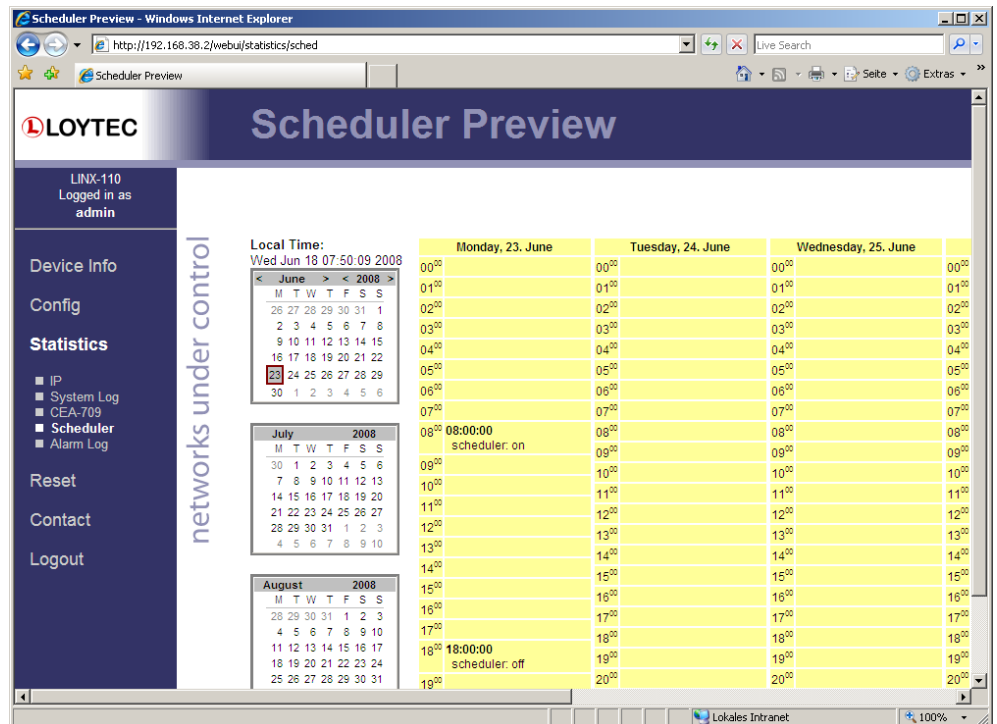


Figure 45: Scheduler Statistics Page.

4.3.8 Alarm Log Page

The alarm log page provides an overview of all alarm logs on the system. Click on one of the links to view a specific alarm log. Each alarm log contains a historical log of alarm transitions. When an inactive and acknowledged alarm disappears from the alarm summary page (live list), the alarm log contains this last transition and maintains it over a reboot. An example is shown in Figure 46.

To refresh the alarm log contents click on the **Reload** button. Currently active alarms cannot be acknowledged in this historical view. Follow the link to the attached alarm objects to get to the respective live lists, where alarms can be acknowledged on the Web interface (see Section 4.2.15).

The alarm log contents can be uploaded from the device in a CSV formatted file. Click on the button **Upload Alarm Log** to upload the current log. To clear the log, press the button **Clear Alarm Log**. Please note, that this permanently purges all historical alarm log data of this alarm log.

Event Time	State	Type	Priority	Description	Source Name	Value	Ack Source	Alarm Time	Clear Time
12.08.2008 21:13:35	acknowledged	low-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	-10.000000	admin@new.LINX-100	12.08.2008 21:12:49	12.08.2008 21:13:35
12.08.2008 21:13:21	acknowledged	high-limit	0	Light Alarm	NV_tn20Controller_1mvl03lux	4000.000000	admin@new.LINX-100	12.08.2008 21:12:56	12.08.2008 21:13:21
12.08.2008 21:12:49	acknowledged	high-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	120.000000	admin@new.LINX-100	12.08.2008 21:12:45	12.08.2008 21:12:49
12.08.2008 21:12:49	acknowledged	low-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	-10.000000	admin@new.LINX-100	12.08.2008 21:12:49	
12.08.2008 21:12:56	active	high-limit	0	Light Alarm	NV_tn20Controller_1mvl03lux	4000.000000	admin@new.LINX-100	12.08.2008 21:12:56	
12.08.2008 21:12:56	active	high-limit	0	Light Alarm	NV_tn20Controller_1mvl03lux	4000.000000		12.08.2008 21:12:56	
12.08.2008 21:12:49	active	low-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	-10.000000		12.08.2008 21:12:49	
12.08.2008 21:12:49	acknowledged	low-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	120.000000		12.08.2008 21:12:45	12.08.2008 21:12:49
12.08.2008 21:12:45	active	high-limit	0	Overheat Alarm	NV_tn20Controller_1mvl01temp	120.000000		12.08.2008 21:12:45	

Figure 46: Alarm Log Page.

4.4 L-WEB

This configuration page provides a download link to the L-Web application installer and a listing of L-Web projects available on the device (see Figure 47). Clicking on **Install** will download the installer for L-Web and start the installation process. See Section 9.2 for more information on working with the L-WEB visualization.

Name	Last modified	Size (Bytes)
room_5.lweb	16.01.2009 14:54:42	137591
room_1.lweb	16.01.2009 14:54:00	137580
room_6.lweb	16.01.2009 15:00:39	137523
room_3.lweb	16.01.2009 14:52:13	137580
room_2.lweb	16.01.2009 14:50:50	137813
office_room.lweb	16.01.2009 12:42:49	170640

Figure 47: L-WEB Page.

4.5 Reset, Contact, Logout

The menu item **Reset** allows two essential operations:

- Rebooting the LINX-10X from a remote location, or

- reset the data point configuration from a remote location. This option clears all data points and the entire port configuration. It leaves the IP settings intact.

The **Contact** item provides contact information and a link to the latest user manual and the latest firmware version.

The **Logout** item closes the current session.

5 Concepts

5.1 CEA-709 OPC Server

The LINX-10X implements an embedded OPC server which exposes network variables (NVs) and configuration properties (CPs) from the CEA-709 network to OPC. The OPC server is based on OPC XML-DA Web service.

The LINX-10X has one physical FT port and one IP-852 port, which is accessible over Ethernet. On the LINX-100, the OPC server node is internally connected either to the FT port or to the IP-852 port. Which one is used can be configured in the CEA-709 configuration (see Section 4.2.5). The schematic is shown in Figure 48 (a). If configured for the FT channel, the LINX-100 provides an RNI for remote access to the FT channel. The RNI can be used to commission nodes and trouble-shoot communications on the FT channel.

The LINX-101 possesses a CEA-709 router, which connects the FT port and the IP-852 port. On the LINX-101 the OPC server node is always internally connected to the FT port. The schematic is shown in Figure 48 (b).

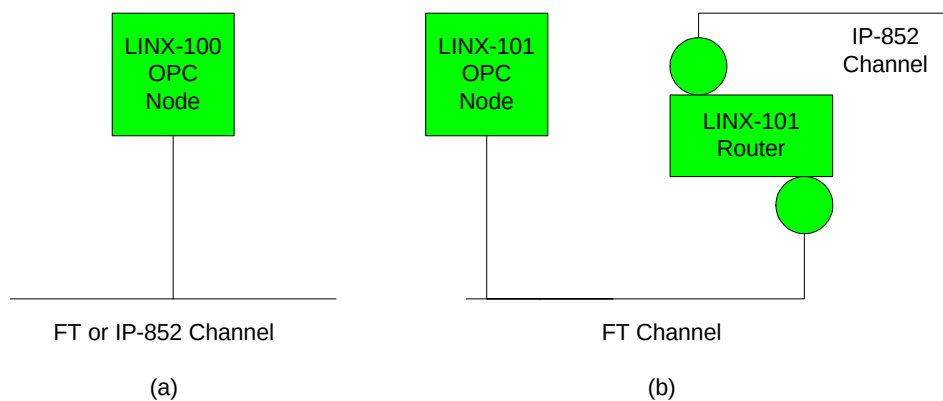


Figure 48: (a) OPC server node on LINX-100, (b) OPC server node and router on the LINX-101.

If the OPC server shall only expose network variables from the local FT channel and there is no IP-852 backbone, then the router is not needed. In this case, the user needs to commission only the OPC node. To attach the FT channel to an IP-852 backbone, the router in the LINX-101 needs to be commissioned. See Chapter 7 for more information on the built-in router and configuration server.

5.2 Data Points

5.2.1 Overview

Data points are part of the fundamental device concept to model process data. A data point is the basic input/output element on the device. Each data point has a value, a data type, a direction, and a set of meta-data describing the value in a semantic context. Each data point also has a name and a description. The entire set of data points is organized in a hierarchy.

At the data point level, the specific technological restrictions are abstracted and hidden from the user. Working with different technologies at this level involves common workflows for all supported technologies.

The direction of a data point is defined as the “network view” of the data flow. This means, an input data point obtains data from the network. An output data point sends data to the network. This is an important convention to remember as different technologies may define other direction semantics.

The basic classes of data points are:

- **Analog:** An *analog* data point typically represents a scalar value. The associated data type is a *double precision* machine variable. Meta-data for analog data points include information such as value range, engineering units, precision, and resolution.
- **Binary:** A *binary* data point contains a Boolean value. Meta-data for binary data points includes human-readable labels for the Boolean states (i.e., active and inactive texts).
- **Multi-state:** A *multi-state* data point represents a discrete set of states. The associated data type is a signed integer machine variable. Each state is identified by an integer value, the *state ID*. State IDs need not be consecutive. Meta-data of a multi-state data point includes human-readable descriptions for the individual states (state texts) and the number of available states.
- **String:** A *string* data point contains a variable-length string. The associated data type is a character string. International character sets are encoded in UTF-8. A string data point does not include any other meta-data.
- **User:** A *user* data points contains un-interpreted, user-defined data. The data is stored as a byte array. A user data point does not include any other meta-data. This type of data point also serves as a container for otherwise structured data points and represents the entirety of the structure.

5.2.2 Timing Parameters

Apart from the meta-data, data points can be configured with a number of timing parameters. The following properties are available to input or output data points, respectively:

- **Pollcycle** (input): The value is given in seconds, which specifies that this data point periodically polls data from the source.
- **Receive Timeout** (input): This is a variation on the poll cycle. When receive timeout is enabled, the data point actively polls the source unless it receives an update. For example, if poll cycle is set to 10 seconds and an update is received every 5 seconds, no extra polls are sent.
- **Poll-on-startup** (input): If this flag is set, the data point polls the value from the source when the system starts up. Once the value has been read, no further polls are sent unless a poll cycle has been defined.
- **Minimum Send Time** (output): This is the minimum time that elapses between two consecutive updates. If updates are requested more often, they are postponed and the

last value is eventually transmitted after the minimum send time. Use this setting to limit the update rate.

- **Maximum Send Time** (output): This is the maximum time without sending an update. If no updates are requested, the last value is transmitted again after the maximum send time. Use this setting to enable a heart-beat feature.

5.2.3 Default Values

Default values can be defined for data points when needed. The value of a data point will be set to the defined default value, if no other value source initializes the data point. Default values are beneficial, if certain input data points are not used by the network and need a pre-defined value, e.g., for calculations. Default values are overridden by persistent values or values determined by poll-on-startup.

5.2.4 Persistency

Data point values are by default not persistent. This means that their value is lost after a power-on reset. There exist different strategies for initializing data points with an appropriate value after the device has started.

For input data points, the value can be actively polled from the network when starting up. Use the Poll-on-Startup feature for this behavior. Polling the network values has the advantage that intermediate changes on the network are reflected. An input data point can be made persistent, if the last received value shall be available after a power-on reset before a poll-on-startup completes. This can be beneficial, if the remote device is temporarily offline and the last value is considered usable.

For output data points, the value can be restored after starting up by the application. For example, if the output data point's value is determined by an input data point and a math object, or the output data point is in a connection with an input, the input can poll its value on startup. If the output data point has no specific other value source, e.g., it is a configuration parameter set by the user, it can be made *persistent*.

To make a data point persistent, enable the Persistent property of the respective data point. The persistency option is only available for the base data point classes analog, binary, multi-state, string and user. More complex objects such as calendars, schedules, etc., have their own data persistency rules.

For structured data points, only all or none of the structure members can be made persistent. The configuration of the top-level data point, which represents the entire structure, serves as a master switch. Setting the top-level data point to be persistent enables persistency for all sub-data points. Clearing it disables persistency for all sub-data points.

5.2.5 Behavior on Value Changes

The value of a data point can change, if it is written by the application or over the network. For all data points (input and output) the application (connection, user control, etc.) can be notified, when the value is written to. The property **Only notify on COV** defines, whether the notification is done with each write or only if the value changes (change-of-value, COV). If only notify on COV is disabled, writing the same value multiple times will result in multiple notifications.

When the value of an output data point is updated, an update is usually sent out onto the network. The property **Send-On-Delta** decides how the update is reflected on the network. If send-on-delta is inactive, each update of the value is sent. If send-on-delta is active, value changes only are sent. The send-on-delta property is only valid for output data points.

For analog data points, the COV or send-on-delta takes an extra argument, which specifies by what amount the value must change to regard it as a change for action. Both, COV and send-on-delta for analog data points check the **Analog Point COV Increment** property. A

change is detected, if the value increment is bigger or equal to the specified increment. If the property is zero, all updates are considered.

5.2.6 Custom Scaling

Custom scaling is applied to all analog data points when they communicate values to or from the network. This feature can be used, if a network data point has engineering units not suitable for the application (e.g., grams instead of kilograms). The scaling is linear and applied in the direction from the network to the application as:

$$A = k N + d,$$

where N is the network value, k the *custom scaling factor*, d the *custom scaling offset*, and A the application value. When sending a value to the network, the reverse scaling is applied. If this property is enabled, the analog values are pre-scaled from the technology to the data point. The custom scaling is in addition to any technology-specific scaling factors and can be applied regardless of the network technology.

5.2.7 System Registers

The LINX-10X provides a number of built-in system registers. They are present without a data point configuration. The system registers, such as the System time or the CPU load, can be exposed to the OPC server. By default, all system registers are checked for being exposed to OPC. To reduce the number of needed OPC tags, you may deselect certain system registers, which are not useful in a specific project.

System register can also serve as a testing setup for the OPC XML-DA communication without a network data point configuration. The *System Time* register is updated every second and may serve for testing subscriptions. The *Authentication Code* register can be used to verify writing to OPC tags.

5.2.8 User Registers

The LINX-10X can be configured to contain user registers. In contrast to system registers, these are only available as a part of the data point configuration. User registers are data points on the device that do not have a specific technological representation on the control network. Thus, they are not accessible over a specific control network technology.

A register merely serves as a container for intermediate data (e.g., results of math objects). The register can have the following, basic data types:

- **Double:** A register of base type *double* is represented by an *analog* data point. It can hold any scalar value. No specific scaling factors apply.
- **Signed Integer:** A register of base type *signed integer* is represented by a *multi-state* data point. This register can hold a set of discrete states, each identified by a signed stats ID.
- **Boolean:** A register of base type *Boolean* is represented by a *binary* data point. This register can hold a Boolean value.

Since a register has no network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input). A suffix is added to the register name to identify the respective data point. For example, the register *MyValue* will have two data points generated for: *MyValue_Read* and *MyValue_Write*.

5.2.9 Math Objects

Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables $v_1, v_2, \dots, v_n$) and calculates a result value according to a specified formula. The result is written to a set of

output data points. The formula is calculated each time one of the input data points updated its value. The formula is only evaluated if all of the input data points have a valid value (i.e., don't show the *invalid value* status).

5.3 Connections

With the use of connections, data points can interact with each other. Connections specify which data points exchange values with each other. Both types of connections - “1:n” and “m:1” connections – are supported. The single data point is referred to as the *hub* data point, whereas the other data points are the *target* data points.

This means, the following connections are possible:

- 1 input data point is connected to *n* output data points,
- *m* inputs data points are connected to 1 output data point.

The most common connection will be the 1:1 connection. This is the type of connection that is auto-generated by the Configurator software. Other types must be created manually in the Configurator.

In the 1:n connection the input value is distributed to all *n* output data points. In the m:1 connection, the most current input value is written to the output data point. When polling the output data point in poll-through mode (maximum cache age is set on the output), the value from the first input data point is polled.

Connections can connect data points of different technologies with each other (also mixed among the target data points) but are restricted to the same class of data points. This means only data points of class *analog* can exchange values within a connection.

For certain classes of data points, additional restrictions exist:

- **Analog:** The value range is capped on the output data points. This means, if the input value in the hub does not fit into the range of an output data point, the value is capped to the biggest or smallest allowed value.
- **Binary:** No special restrictions exist.
- **Multi-state:** Only multi-state data points of an equal number of states can be placed into a connection. The actual state IDs need not be equal. They are ordered and the *n*-th state is propagated over a connection. For example, the 2nd state on the hub has the state ID ‘2’, while on the target the 2nd state has the state ID ‘0’.
- **String:** No special restrictions exist.
- **User:** Only user data points of the same length can be placed in a connection.

5.4 AST Features

5.4.1 Alarming

The alarming architecture comprises a number of entities. Objects that monitor values of data points and generate alarms depending on an *alarm condition* are called *alarm sources*. The alarms are reported to an *alarm server* on the same device. The alarm server maintains a list of alarm records, called the *alarm summary*. The alarm server is the interface to access the local alarms. This can be done over the network or the Web UI.

An alarm record contains the information about the alarm. This includes information about the alarm time, the source of the alarm, an alarm text, an alarm value, an alarm type, an

alarm priority, and an alarm state. An alarm record undergoes a number of state changes during its life-cycle. When the alarm occurs, it is *active*. When the alarm condition subsides, the alarm becomes *inactive*. Active alarms can be acknowledged by an operator. Then they become *active acknowledged*. Active alarms can also become inactive, but an acknowledgement is still required. Then they become *ack-pending*. When an alarm is inactive and was acknowledged it disappears from the alarm summary.

Other devices can access the alarm information of an alarm server. These devices are *alarm clients*. They register with the alarm server and get notified about changes to the alarm summary. Alarm clients can be used to display the current alarm summary and acknowledge alarms.

Depending on the underlying technology, some restrictions to the available alarm information and acknowledgement behavior may exist.

5.4.2 Historical Alarm Log

The alarm summary of the alarm objects contains a live list of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* is utilized. An alarm log can log transitions of one or more alarm objects.

The alarm log is always local and stored as a file on the device. The size of an alarm log is configurable. The alarm log operates as a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by newer alarm transitions. The alarm log is available on the Web UI or can be uploaded from the device as a CSV file. The CSV file can also be used as an e-mail attachment.

5.4.3 Scheduling

Schedulers are objects that schedule values of data points on a timely basis. A scheduler object is configured by which data points it shall schedule. This configuration is done by the system engineer once, when the system is designed. The configuration of the times and values that shall be scheduled is not part of that initial configuration and may be changed later. This distinction has to be kept in mind.

A scheduler object sets its data points to predefined values at specified times. The function of the scheduler is state-based. This means, that after a given time, the scheduler maintains this state. It can re-transmit the scheduled values as appropriate (e.g., when rebooting). The predefined values are called *value presets*. A value preset contains one or more values under a single label (e.g., “day” schedules the values { 20.0, TRUE, 400 }).

Which value preset is scheduled at what time is defined through a *daily schedule*. The daily schedule defines the times and value presets in a 24-hour period. A schedule typically contains daily schedules for the weekdays Monday through Sunday. See Figure 49 for an example of a daily schedule.

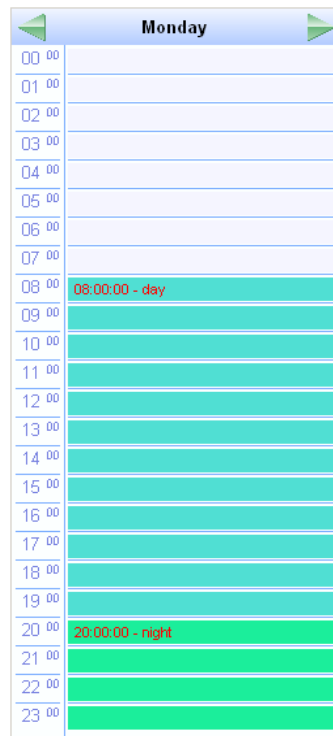


Figure 49: Example of a Daily Schedule.

For some tasks the daily schedules on weekdays is sufficient. However, on some specific dates, there may be exceptions to the regular week. This can be implemented by defining daily schedules for *exception days*. For instance, there may be a separate daily schedule for *Holidays*. The exception days are defined through a *calendar*. The calendar contains a number of *calendar patterns*. Each calendar pattern describes a pattern of dates that define the class of an exception, e.g., *Holidays*.

When a calendar is defined on a system, the exception days are available in all schedules. When a schedule wants to define daily schedules for some of the available exception days, they need to be enabled in the schedule. See Figure 50 for an example where *Holidays* is used.

Weekly / Exception Schedule Configuration			
Weekday / Exception	Priority	Events	Use
Mon	-	2	☒
Tue	-	0	☒
Wed	-	0	☒
Thu	-	0	☒
Fri	-	0	☒
Sat	-	0	☒
Sun	-	0	☒
24_12_xx	0 (highest)	0	☐
Holiday	126 (lowest)	0	☒
Maintenance Days	126 (lowest)	0	☐

Figure 50: Example of used Exception Days.

The function of the exception is simple. The daily schedule of a regular weekday is overridden by the daily schedule of the exception, when one of the specified date patterns is in effect (e.g., July 14th in Holidays overrides the regular weekday). If more than one exception days are in use, there may be conflicts on specific dates. These conflicts are resolved by defining *priorities* for the different exceptions. The daily schedule of the exception with the higher priority is eventually in effect. If two exceptions with the same priority exist, it is not defined, which one is in effect. Therefore, always use distinct priorities.

Apart from the defined value presets, there exist special events that can be scheduled in a daily schedule. They affect how the scheduler behaves and which exception is active:

- **Invalid:** If this value is scheduled, the scheduler transmits the invalid value. The numeric representation of that invalid value is defined by the underlying data point and is technology-specific.
- **Withdraw:** If this value is scheduled, the scheduler takes the previously value preset out of effect. This means that the daily schedule with the next lower priority becomes effective. If no daily schedule with lower priority applies, the scheduler behaves as if it was disabled. Figure 50 presents an example of the *Maintenance Day* exception day, which schedules the *maint* value at 6 am and goes out of effect at 10 am. If the maintenance day falls on a Monday, the regular schedule for Monday will be overridden by the Maintenance schedule at 6 am and become effective again at 10 am sending the *day* value.
- **Temporary Disable:** If this value is scheduled, the entire scheduler is disabled until a new event is scheduled in a daily schedule of the same or higher priority than the one that has the temporary disable event. This type of event can be used to define periods for manual override.

Please also refer to the technology-specific limitations described in Section 6.11 to learn about special behavior of the respective networking technology.

Maintenance Days	Monday	Result
00 00	00 00	00 00
01 00	01 00	01 00
02 00	02 00	02 00
03 00	03 00	03 00
04 00	04 00	04 00
05 00	05 00	05 00
06 00	06 00	06:00:00 - maint
07 00	07 00	07 00
08 00	08 00	08 00
09 00	09 00	09 00
10 00	10 00	10:00:00 - day
11 00	11 00	11 00
12 00	12 00	12 00
13 00	13 00	13 00
14 00	14 00	14 00
15 00	15 00	15 00
16 00	16 00	16 00
17 00	17 00	17 00
18 00	18 00	18 00
19 00	19 00	19 00
20 00	20 00	20:00:00 - night
21 00	21 00	21 00
22 00	22 00	22 00
23 00	23 00	23 00

Figure 51: Example using withdraw in an exception schedule.

The configuration of exceptions is done by calendar patterns in the calendar. Each calendar pattern contains a number of pattern entries. These entries can define the following:

- A single date: This defines a single date. Wildcards may be used in the year to specify July 14th of every year.
- A date range: This defines a range. Starting with a start date and ending with the end date. No wildcards should be used.

- A Week-and-Day definition: This defines dates based on a week, such as every 1st Friday in a month, every Monday, every last Wednesday of a month.

While exception days of a calendar are accessible to all schedules on a device, specific exceptions can be defined, which are embedded into a specific schedule. These are referred to as an *embedded calendar*. In contrast to a regular calendar each calendar pattern of an embedded calendar can hold exactly one date entry. This can be a single date or a date range. The embedded exception days are only visible to the schedule they are defined in. Apart from these restrictions, embedded calendars behave like the regular calendar. Figure 50 shows an example for an embedded exception day named '24_12_xx'.

A schedule defines at which time instants certain states of the scheduled data points are maintained. The *next-state* feature allows looking ahead into the future and predicting when the next scheduled state will occur. There are two data points involved: the time-to-next-state is a counter in minutes to the next scheduled event, and the next-state data point is the state of the next scheduled event. This information can be used by controllers to optimize their algorithms (e.g., pre-heat a room for the scheduled occupancy state). Use the `SNVT_tod_event` in CEA-709 to accomplish this task.

When a scheduler is executing the schedule on the local device, it is called a *local scheduler*. Such a scheduler is configured to schedule data points and later its daily schedules can be modified. When accessing the daily schedules of a scheduler, which executes on a remote device, the object is called a *remote scheduler*. A remote scheduler has the same interface to the user to modify daily schedules. A remote scheduler object can be used as a user-interface for schedulers that execute on different devices.

5.4.4 Trending

Trending refers to the ability to log values of data points over time. A trend log object is responsible for this task. It is configured, which data points shall be trended. Log records are generated either in fixed time intervals, on change-of-value conditions, or when a trigger is activated. Trend log objects can trend either local or remote data points.

The trend data is stored in a binary format on the device. The capacity of a given trend log is configured. The trend log can be operated in one of two modes: (1) In linear mode the trend file fills up until it reaches its capacity. It then stops logging. (2) In ring buffer mode. In this mode the oldest log records are overwritten when the capacity is reached.

Trended data points can be logged as their actual values at given time instants or as an aggregated value over the defined log interval. Aggregation can be calculated as minimum, maximum, or average. Aggregation can be beneficial, if the trended value changes more frequently than the selected log interval. Using aggregation, the log interval can be chosen to limit the amount of logged data while preserving information of the trended value.

How many data points can be trended in one trend log is limited by the underlying technology. So are some of the log modes. Refer to the technology sections for more information.

5.4.5 E-mail

The e-mail function can be combined with the other AST features. The format of an e-mail is defined through *e-mail templates*. An e-mail template defines the recipients, the e-mail text, value parameters inserted into the text and triggers, which invoke the transmission of an e-mail. An e-mail template can also specify one or more files to be sent along as an attachment.

A prerequisite to sending e-mails is the configuration of an e-mail account on the LINX-10X. This can be done on the Web UI (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**). It is recommended to use the e-mail server of your Internet provider. For public mailers, enable the required authentication. Please note that the LINX-

10X does currently not support the SS/TLS e-mail authentication mechanism. Therefore, Hotmail and gmail cannot be used.

The amount of generated e-mails can be limited using a rate limit algorithm. The transmission of e-mails can be disabled altogether by using a special data point. That data point can be scheduled or driven over the network.

If an E-Mail cannot be sent (e.g. the mail server is not reachable), the mail delivery is retried up to 24 times every 30 minutes.

5.5 CEA-709 Technology

5.5.1 CEA-709 Data Points

Data points in the CEA-709 network are known as network variables (NVs). They have a direction, a name, and a type, known as the standard network variable type (SNVT) or user-defined network variable type (UNVT). In addition to NVs, also configuration properties (CPs) in the CEA-709 network can be accessed as data points. Both standard CP types (SCPTs) and user-defined CP types (UCPTs) are supported.

The typical procedure in configuring the LINX-10X consists of the following steps:

1. Select the data points of the network to be used on the LINX-10X (e.g., select the NVs in the CEA-709 network nodes)
2. Create necessary registers, math objects
3. Select those data points on the LINX-10X, which shall be exposed as OPC tags

The CEA-709 NVs on the LINX-10X can be created in three different ways:

- **Static NV:** For each selected NV on the network there is a static NV created on the LINX-10X. This NV can be bound to the NV on the network. Note that adding static NVs to the LINX-10X results in a change to the default XIF file. The LINX-10X is assigned a new “model number” to reflect this change (see Section 5.5.2). Static NVs are the way to use NVs in non-LNS systems, where NVs shall be bound instead of using polling.
- **Dynamic NV:** For each selected NV on the network there is a dynamic NV created on the LINX-10X. Compared to static NVs, dynamic NVs do not change the XIF interface of the LINX-10X. The dynamic NVs are created by the network management tool. Currently, only LNS-based tools can manage dynamic NVs. As for static NVs, with dynamic NVs it is possible to use bindings instead of polling.
- **External NV:** The selected NVs on the network are treated as external NVs to the LINX-10X. The LINX-10X doesn’t create any NVs on the device, but instead uses polling to read from those NVs and explicit updates to write to the NVs. Therefore, no bindings are necessary for external NVs. For input data points using external NVs however, a poll cycle must be configured. If not configured explicitly, a default poll cycle of 10 sec. is chosen. The default poll cycle can be changed in the project settings menu.

Based on the NV the data point is derived from, the following kinds of data points are created:

- Simple NVs that hold only one scalar value, e.g., SNVT_amp: Those kinds on NVs are represented as analog data points. The data points holds the current value, NV scaling factors are applied.

- Simple NVs based on an enumeration, e.g., SNVT_date_day: Enumeration types result in multi-state data points. They represent the state of the NV.
- Structured NVs that consists of a number of fields, e.g., SNVT_switch: All structured NVs are represented as user point. That is, the data point is structured similar to the NV it is based on. Beneath the user data point, the individual structure fields are presented as “sub-data points”.

For more information on the different types of network variables and their implications please refer to the application note in Section 16.2. For CPs the allocation type “File” is used.

5.5.2 Static Interface Changes

The LINX-10X can be configured to use static NVs. Unlike dynamic NVs, static NVs cannot be created in the network management tool. They are part of the static interface and are usually compiled into the device. When static NVs are used, the LINX-10X changes its static interface and boots with a new one.

Each time the static interface of the LINX-10X changes (i.e., static NVs are added, deleted, or modified), the model number is changed. The model number is the last byte of the program ID. Thus, a change in the static interface results in a change of the program ID and a new device template needs to be created in the network management tool. A new device template usually means that the device has to be deleted and added again in the database. All bindings and dynamic NVs have to be created again for the new device.

When the LINX-10X Configurator is connected via LNS, it supports the process of changing the device template for the new static interface. It automatically upgrades the device template of the LINX-10X device in the LNS database and restores the previous bindings and dynamic NVs. If the LINX-10X is not configured with an LNS-based tool, this support is not available. The new static interface is only available in a new XIF file or by uploading the new device template into the database. For more information on the static interface and device templates please refer to the application note in Section 16.2.

6 The LINX-10X Configurator

This Chapter gives step-by-step instructions on how to commission LINX-10X, create a data point configuration with input and output network variables, and how to expose those data points to the OPC server. We show the configuration steps using LonMaker TE but other LNS-based network management tools can be used as well to install and configure the LINX-10X. We also show how to configure the LINX-10X without LNS.

6.1 Installation

6.1.1 Software Installation

The LINX-10X Configurator must be used to setup the data point configuration of the LINX-10X. The Configurator is installed as a plug-in tool for all LNS-based network management tools as well as a stand-alone tool (for systems without LNS).

System requirements:

- LNS 3.1, Service Pack 8 or LNS TE SP5 or higher (for LNS mode),
- Windows XP, Windows 2003 Server, Windows Vista, Windows 7, or Windows 2008 Server.

The LINX-10X Configurator can be downloaded from the LOYTEC Web site <http://www.loytec.com>. When asked for the type of installation, there are two options to choose from. Select **Typical** to install the required program files. Select **Full** to install the LONMARK resource files along with the software. This option is useful, when the system does not have the newest resource files.

6.1.2 Registration as a Plug-In

If the LINX-10X shall be configured using LNS-based tools (e.g., NL200 or LonMaker), the LINX-10X Configurator needs to be registered as an LNS plug-in. In the following, the process is described for LonMaker TE. Otherwise, please refer to the documentation of your network management tool on how to register an LNS plug-in.

To Register in LonMaker TE

1. Open LonMaker and create a new network.
2. Click **Next** until the plug-in registration tab appears in the Network Wizard. Select the **LOYTEC LINX-100 Configurator (Version X.Y)** from the list of **Not Registered** (see Figure 52).

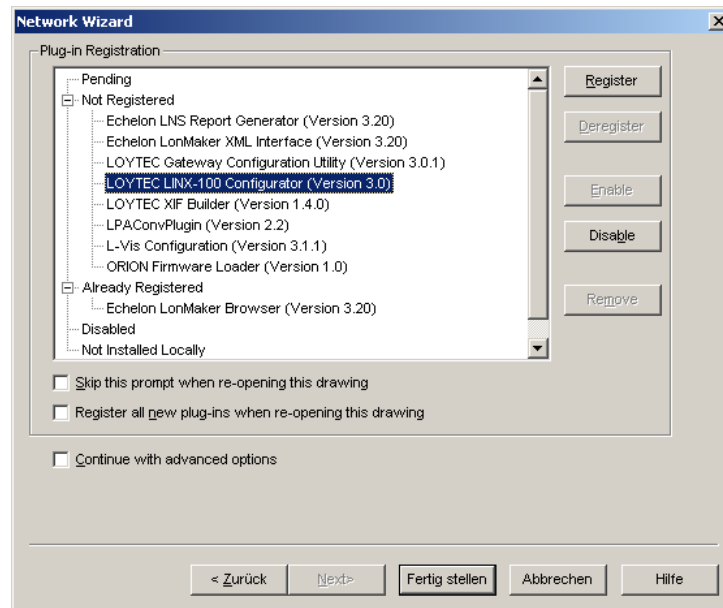


Figure 52: Select the Plug-in to be registered.

3. Click **Register**. The Configurator now appears in the **Pending** list.
4. Click **Finish** to complete the registration. Device templates for the LINX-10X are added automatically and XIF files are copied into the LNS import directory.

Note: If you are using multiple databases (projects) make sure you have registered the plug-in in each project.

5. Under **LonMaker** → **Network Properties** → **Plug-In Registration** make sure that the **LOYTEC LINX-100 Configurator (Version X.Y)** shows up under **Already Registered**.

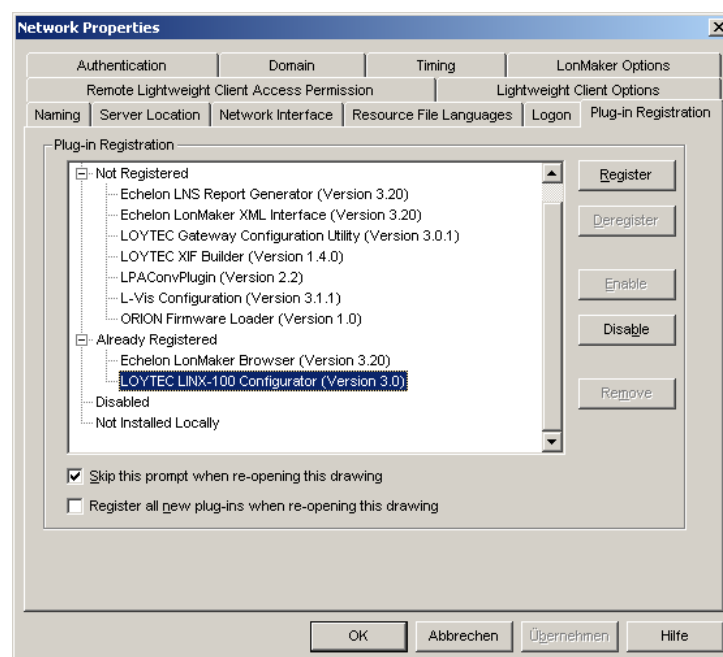


Figure 53: Check that the LINX-10X Configurator is properly registered.

6.1.3 Operating Modes

The Configurator can be used in on-line, off-line, and stand-alone mode. On-line and off-line mode refers to the 2 operating modes of your LNS network management software.

- **On-line Mode:** This is the preferred method to use the configuration utility. The network management tool is attached to the network and all network changes are directly propagated into the network. This mode must be used to add the device, commission the device, extract the port interface definition, and download the configuration into the device.
- **Off-line Mode:** In off-line mode, the network management software is not attached to the network or the device is not attached to the network, respectively. This mode can be used to add the device using the device templates, create the port interface definition and to make the internal connections.
- **Stand-alone Mode:** The Configurator can also be executed as a stand-alone program. This mode is useful for the engineer who doesn't want to start the configuration software as a plug-in from within network management software (e.g., NL-220, LonMaker or Alex). Instead the engineer can work directly with the device when online or engineer it offline.

6.2 Data Point Manager

The Configurator uses a central concept to manage data points. The data point manager is located on the **Datapoints** tab as shown in Figure 54. It is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (number 1 in Figure 54),
- The data point list (number 2 in Figure 54),
- And a property view (number 3 in Figure 54).

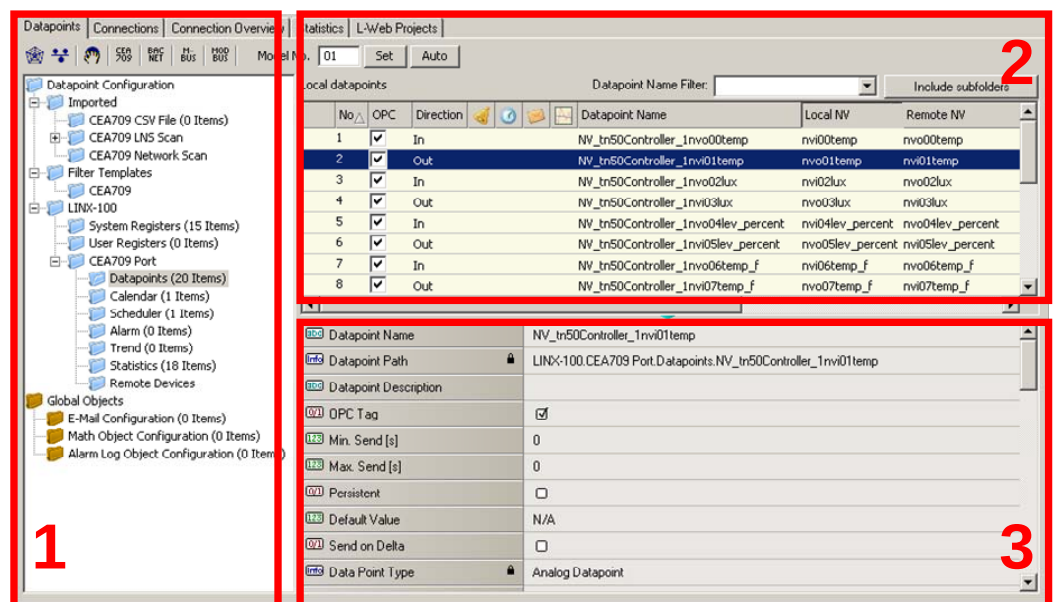


Figure 54: Data Point Manager Dialog.

6.2.1 Folder List

At the left is a list of folders which is used to sort the available data objects by their category. There are a number of predefined folders available:

- **Imported:** This folder has a number of sub-folders for different import methods:
 - o **CSV Import:** This folder is used to display data points imported from CSV files.
 - o **LNS Database Scan:** This folder is used to hold data retrieved from a network database scan.
 - o **CEA709 Network Scan:** This folder holds NVs scanned online from an attached CEA-709 network.

Data objects in the import folder are not stored on the device when the project is downloaded. They represent data objects which are available on remote devices and are shown here as templates to create suitable data objects for use on the device by selecting the **Use on Device** option.

- **CEA709 Templates:** This folder contains the created data point templates. They contain a set of properties, which are applied to CEA-709 data points, when they are created on the LINX-10X.
- **LINX-10X:** This is the device folder of the LINX-10X. It contains all the necessary data points which constitute to the LINX-10X's port interface definition. These data points are created on the LINX-10X when the configuration is downloaded. The three subfolders represent
 - o **System Registers:** This folder contains system registers, which provide information on the device itself.
 - o **User Registers:** This folder holds user-definable registers. These registers are not visible on the underlying network and are intended for internal usage.
 - o **CEA-709 Port:** This folder contains data points, schedulers, calendars, trend logs, statistics, and remote data points of the CEA-709 network technology. See Section 6.2.2.
- **Global Objects:** This top-level folder contains sub-folders that organize specific application objects that operate on data points.
 - o **E-mail Configuration:** This folder contains e-mail templates. An e-mail template defines the destination address and text body of an e-mail, which is triggered by data points and may contain data point values or file attachments. To create an e-mail template, select the folder and use the context menu.
 - o **Math Objects Configuration:** This folder contains math objects. Math objects are used to perform a predefined calculation on a number of input data points and write the result to a defined set of output data points. Each math object contains one formula. To create a math object, select the folder and use the context menu.
 - o **Alarm Log Configuration:** This folder contains the alarm log objects. Each alarm log object creates a historical log of alarm transitions of one or more alarm objects (alarm server or client). To create an alarm log, select the folder and use the context menu.

Using the context menu on a folder, sub-folders may be created to organize the available objects. If new objects are created automatically, they are usually placed in the base folder and can then be moved by the user to any of his sub-folders. Note, that the folder structure described above cannot be changed by adding or deleting folders at that level.

6.2.2 Network Port Folders

Each network port folder on the device has the same structure of sub folders. These sub folders are:

- **Datapoints:** This folder holds all data points, which are allocated on the network port. To create a data point, select the folder and use the context menu.

- **Calendar:** This folder is used to hold a locally available calendar object with its calendar patterns (definitions of day classes like holiday, maintenance day, and so on). Current devices allow one local calendar object. To create a calendar, select the folder and use the context menu.
- **Scheduler:** This folder is used for local scheduler objects. Each of these objects will map to a local scheduler on the device's network port. Configuring schedules through these objects actually transfers *schedule configuration data* to the underlying scheduler objects on the network port. To create a scheduler, select the folder and use the context menu.
- **Alarm:** This folder is used for local alarm server objects. Each of these alarm server objects represent an alarm class, which other objects can report alarms to. Other devices can use the alarm server object to get notified about alarms. To create an alarm server object, select the folder and use the context menu.
- **Trend:** This folder is used for local trend log objects. Each of these objects will be able to trend data points over time and store a local trend log file. To create a trend log object, select the folder and use the context menu.
- **Statistics:** This folder contains registers, which provide communication statistics specific to the network port.
- **Remote Devices:** This folder is used to collect all remote calendars, schedulers, trend logs, and alarm client objects, which were created from network scan data. For each remote device, a subfolder will be created where the objects referencing this device are collected.

6.2.3 Data Point List

At the top right, a list of all data objects which are available in the selected folder is shown. From this list, objects may be selected (including multi-select) in order to modify some of their properties. Click on the **Include Subfolders** button to show all data points of the selected data point folder and all its sub-folders. This can be a convenient way for multi-select across folders. To filter for data point names, enter a search text into the **Datapoint Name Filter** text box and hit *Enter*. A drop-down list holds the previously used filters available.

The list can be sorted by clicking on one of the column headers. For example, clicking on the **Direction** column header will sort the list by direction. Other columns display data point name, NV name, and SNVT. To apply the current sort order as the new data point order on the device, right-click on the column header and select **Renumber Datapoints**. Alternatively, select from the menu **Tools → Renumber Datapoints**.

The **OPC** column provides check boxes for each data point. If checked, the respective data point is exposed to OPC on the device. Deselect the check box, if a data points shall not be exposed to OPC. Note, that deselected data points do not add to the OPC tag limit.

New objects may be created in the selected folder by pressing the **New** button to the right of the list or via the **New** command in the context menu. A plus  sign in the list indicates that the data point contains sub-points. These can be structure members for structured SNVTs. Clicking on the plus  sign expands the view.

For the alarming, scheduling, trending (AST) features, there are columns, which display icons for data points that are attached to an AST function. See Table 7 for details.

Icon	Data Point Usage
	Data point is scheduled
	Data point has an active alarm condition
	Data point has an inactive alarm condition.
	Data point is a trigger for e-mails
	Data point used for trending

Table 7: Icons for used data points in the data point list view.

6.2.4 Property View

When one or multiple data points are selected, the available properties are displayed in the property view. Properties which are read-only are marked with a lock  sign. When applying multi-select, only those properties common to all selected data points are displayed. Depending on the network technology and data point class, different properties may exist.

Data point properties common to all technologies:

- **Datapoint Name:** This is the technology-independent data point name. This name may be longer than and different to the name of the native communication object (i.e., network variable). Data point names must be unique within a given folder. The maximum length is limited to 64 ASCII characters.
- **Datapoint Path:** This informational property specifies the entire path of the data point within the data point hierarchy. The maximum length is limited to 64 ASCII characters.
- **Datapoint Description:** This is a human-readable description of the data point. There are no special restrictions for a description.
- **OPC Tag:** If enabled, the data point will be exposed to OPC. If not enabled, this data point does not contribute to the limit of OPC tags.
- **Use Polycle value as:** For input data points, this property defines whether the input shall use a receive timeout or be constantly polling. See Section 5.2.2.
- **Poll on Startup:** For input data points this property defines, whether the data point shall be polled once at start-up. Poll-on-startup can be enabled independently of the poll cycle. See Section 5.2.2.
- **Pollcycle:** For input data points, this property defines the poll cycle in seconds. Set this property to 0 to disable polling. See Section 5.2.2.
- **Receive Timeout:** For input data points, this property defines the receive timeout in seconds. Set this property to 0 to disable polling. See Section 5.2.2.
- **Min Send:** For output data points, this property defines the min send time in seconds. See Section 5.2.2.
- **Max Send:** For output data points, this property defines the max send time in seconds. See Section 5.2.2.
- **Send-on-delta:** For output data points this property defines, if value updates shall be sent only once they meet the COV condition of the data point. For analog data points the analog COV increment is used. If not checked, updates are always transmitted according to min and max send times. See Section 5.2.6.
- **Use Linear Scaling:** If this property is enabled, the analog values are pre-scaled from the technology to the data point. This scaling is in addition to any technology-specific

scaling factors. If enabled, the properties **Custom Scaling Factor** and **Custom Scaling Offset** accept the scaling factors. See Section 5.2.6.

- **Custom Scaling Factor, Custom Scaling Offset:** These properties only exist, if linear scaling is enabled. They apply to analog data points only. See Section 5.2.6.
- **Only notify on COV:** This property assists for binary and multi-state input data points. It defines, if a data point shall trigger an update only when the value changes or on every write. If this is enabled, consecutive writes with the same value do not trigger an update. If you want to convey every write, disable COV on the data point.
- **Persistent:** This property defines, if the last written value shall be stored as a persistent value. Persistent data points restore that value after a restart from the persistent storage. See Section 5.2.4.
- **Default Value:** This property defines a default value (see Section 5.2.3). Enter a default value to enable this feature in the data point. Delete the value entirely to remove the default value. If no default value is defined, this property reads “N/A”. The default is no default value.
- **Point Type:** This is the base data point type, e.g., “Analog Datapoint”.
- **Direction:** This is the data point direction. Use input or output as directions.
- **Unit Text:** For analog data points this property contains a human-readable text for the engineering units of the scalar value, e.g., “kilogram”.
- **Analog Datapoint Max Value:** For analog data points this property contains the upper limit of the supported value range. Note that this does not define an alarm limit.
- **Analog Datapoint Min Value:** For analog data points this property contains the lower limit of the supported value range. Note that this does not define an alarm limit.
- **Analog Datapoint Precision:** For analog data points this property defines the number of decimals. ‘0’ specifies an integer value. Display units may use this to format the floating point value accordingly.
- **Analog Datapoint Resolution:** For analog data points this property defines the smallest possible value increment.
- **Analog Point COV Increment:** This property is valid for analog input data points. It specifies by which amount the value needs to change, before an update is generated. If every write shall generate an update even when the value does not change, specify 0 as the COV increment. If any value change shall generate an update, delete the value, which results in **Any**.
- **Active Text:** For binary data points this property defines a human-readable text for the active state (true).
- **Inactive Text:** For binary data points this property defines a human-readable text for the inactive state (false).
- **State Count:** For multi-state data points this property defines the number of discrete states. The state count can be changed in the multistate map manager (see Section 6.2.5).
- **State Text:** For multi-state data points this property defines a human-readable state label for each state. The texts can be changed in the multistate map manager (see Section 6.2.5).

6.2.5 Managing Multistate Maps

Multistate data points have a descriptive set of state texts for their state IDs. To manage those state IDs and state texts among many multistate data points, they refer to *multistate maps*. Some technologies have a fixed set of such multistate maps others have freely configurable multistate maps (e.g. user registers). Editing a multistate map affects all

multistate data points, which are using that particular map. It is not necessary to edit each data point individually.

To Edit a Multistate Map

1. Click on the  button in the State Count property of a multistate data point. This opens the multistate map manager as shown in Figure 55.

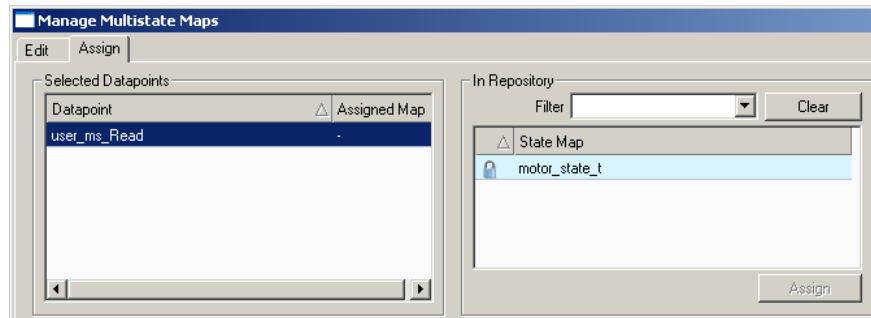
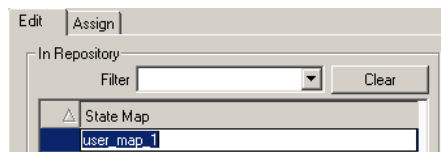
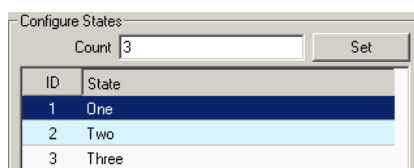


Figure 55: Assign multistate maps in the multistate map manager.

2. Select an existing state map in the **State Map** list and click on **Assign**. Maps that are fixed and cannot be changed are marked with a lock symbol .
3. If a new multistate map shall be created, change to the **Edit** tab.
4. Click on the **Create** button and enter a new multistate map name. Then hit **Enter**.



5. In the **Configure States** box enter the desired number of states and click **Set**.
6. Edit the state texts as needed.



7. Change back to the **Assign** tab.
8. Select the newly created multistate map and click the **Assign** button. The assigned map is now displayed next to the data point.



6.2.6 CEA-709 Properties

Apart from the common data point properties discussed in Section 6.2.4 the data points of the CEA-709 technology have additional properties. Depending on if a NV is local or external (remote), the properties may vary,

- **NV Allocation:** This property defines how a data point shall be allocated on the device. Choices are “Static NV”, “Dynamic NV”, and “External NV”. If the allocation type cannot be changed, this property is locked.
- **SNVT:** This property defines the SNVT of the NV, e.g., “lux (79)”.
- **Invalid Value:** This property defines the “invalid value” for the NV. If set, this specific value will be interpreted as “invalid” in the data point. If known by the SNVT, the invalid value is filled in. Otherwise, the user can specify an invalid value.
- **CEA-709 Mapping Information:** This information is derived from the SNVT. It defines how the NV contents are mapped to the data point.
- **NV Scaling A, B, C:** These are the scaling factors known from the SNVT table. The scaling factors are applied to translate a raw NV value into the scalar representation of the data point.
- **Data Type:** This is the basic NV data type. This is usually filled in from the SNVT definition.
- **Local NV Member Index:** This property specifies the NV member index within a given functional block. This must be a unique index in the functional block, which identifies the NV after other NVs have been added or removed from the interface.
- **Local/Remote NV Index:** This property specifies the NV index. For local, static NVs this is the NV index of the static NV. For external NVs, this is the NV index of the NV on the remote device.
- **Local/Remote NV Name:** This property specifies the programmatic name of the NV. For local, static NVs this is the programmatic name of the static NV. For external NVs, this is the programmatic name of the NV on the remote device.
- **Local/Remote Functional Block:** This property specifies the programmatic name of the NV. For local, static NVs, one of the reserved functional blocks can be selected.
- **Local/Remote NV Flags:** This property specifies the NV flags. For local (static or dynamic) NVs, the flags can be configured. For external NVs, these flags are only informational.
- **Remove NV Information:** For external NVs, this property contains the information on the remote device and the NV selector on that device.
- **Remote Device ID:** For external NVs, this property contains information on the remote device by listing the program ID and location string.
- **Remote Device Address:** For external NVs, this property contains the CEA-709 network addressing information to access the node, i.e., subnet, node, and NID.
- **Retry Count:** For external NVs, this property defines the retry count. The default is 3.
- **Repeat Timer:** For external NVs, this property defines the repeat timer in milliseconds. The default is 96 ms.
- **Transmit Timer:** For external NVs, this property defines the transmit timer in milliseconds. The default is 768 ms.
- **LNS Network Path:** If available from an LNS scan, this property specifies the LNS network path of the device where the given NV exists.
- **LNS Channel Name:** If available from an LNS scan, this property specifies the LNS channel name of the device where the given NV exists.

6.3 Project Settings

The project settings allow defining certain default behavior and default settings used throughout the project. To access the project settings go to the menu **Settings → Project Settings...**. This opens the project settings dialog, which provides several tabs as described in the following sections.

6.3.1 General

The general tab of the project settings as shown in Figure 56 contains settings independent of the technology port. The settings are:

- **Project Name:** This setting allows entering a descriptive name for the project.
- **Default FTP Connection Settings:** Enter a user name and password for the default FTP access. This access method is used implicitly when connected via LNS and the device is accessible over IP. For this implicit connection, there is no dialog to ask for a username and password and the username and the default password from the project settings are used.
- **Device Configuration Download Default:** This group of settings defines, how the download of device configuration parameters shall proceed. If **Do not download** is selected, the configuration download does not download anything else than the data point configuration. If **Ask** is selected, the download will pop up a dialog in which the user can choose what to download. If **Download specific** is selected, the project settings of this dialog determine what is downloaded onto the device. As a default, the configuration download includes the schedules and calendar patterns but does not include the device settings as defined in the **Device Configuration** tab (see Section 6.3.5).
- **Automatically add downloaded device to the OPC Bridge:** This option is only available, if LOPC-BR800, the LOYTEC OPC bridge software, is installed on the same PC. If enabled, the LINX-10X device, a configuration is downloaded to, is automatically added to the OPC server list in the bridge. For more information on using LOPC-BR800 refer to Section 9.3.
- **Automatically structure imported data points for faster OPC browsing:** This option enables the automatic generation of sub-folders when using data points on the device. A sub-folder is created for each scanned or imported device. This allows OPC clients to browse the OPC tags in a hierarchical way.

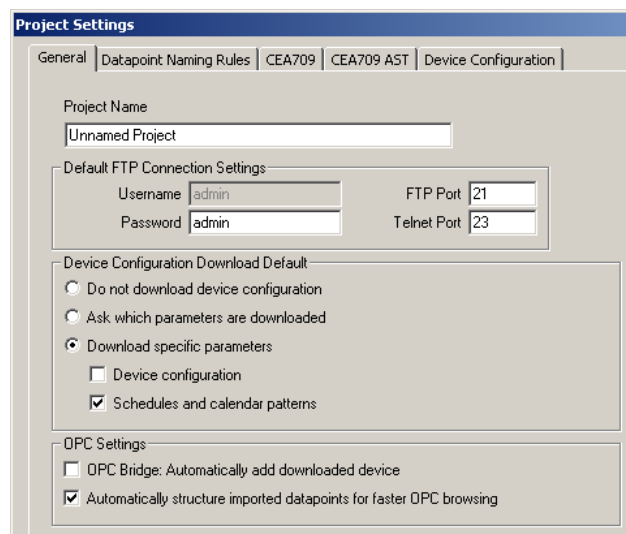


Figure 56: General Project Settings.

6.3.2 Data Point Naming Rules

The data point naming rules tab (see Figure 57) allows specifying how data point names are automatically derived from scanned network variables. The preview shows how names would look like, when the check marks are modified.

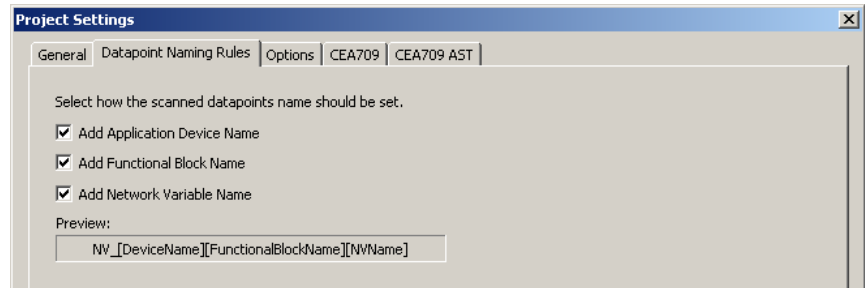


Figure 57: Data Point Naming Rules Project Settings.

6.3.3 CEA-709 Settings

The CEA-709 configuration tab as shown in Figure 58 allows configuring properties of the device's CEA-709 port. The options are:

- **Enable Legacy Network Management Mode:** This group box contains check boxes for each CEA-709 port of the device. Put a check mark on the port, if this port shall be operated in the legacy network management mode. In that mode, the port does not use the extended command set (ECS) of network management commands. This can be necessary to operate the device with some network management tools that do not support the ECS.
- **Default Pollcycle for External NVs:** When using external NVs, this poll cycle is set as a default for input data points. The poll cycle can be edited individually in the properties view of the data point manager.
- **Use state-member of SNVT_switch as:** This setting defines how the state member of the SNVT_switch shall be mapped to a data point. Depending on how the data point shall be used, it can be binary or multi-state. The multi-state setting allows setting the UNSET state explicitly. As a binary point the UNSET state is implicitly chosen, if the value is invalid.
- **Omit unused child data points of UNVT/UCPT structures:** This setting defines, that if set, also unused sub-data points of user-defined structure types are not downloaded onto the device. This option can reduce the total amount of data points in the configuration. As a default it is not enabled to allow full structure information after an upload to the PC even if the user does not have the original resource files installed.
- **Configuration Download:** This group box contains self-configuration settings for the CEA-709 ports. This is necessary if the device shall be used without being commissioned by a network management tool. Set the check mark and enter the CEA-709 domain and subnet/node information. If operated in self-configured mode, the CEA-709 network can be scanned using the network scan (see Section 6.7.6) and external NVs can be used on the device. Note, that the domain must match the nodes' domain on the network and the subnet/node address must not be used by another device.

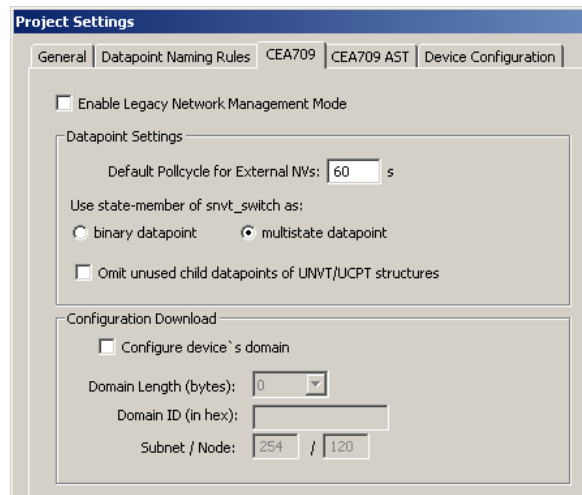


Figure 58: CEA-709 Project Settings.

6.3.4 AST Settings

For CEA-709 devices, the use of alarming, scheduling, and trending (AST) features requires additional resources (functional objects and NVs). This changes the static interface. Since the number of used resources also influences the performance, the CEA-709 AST tab allows configuring those resources for the project. In this tab, the required number of scheduler units that may be instantiated and their capacity may be configured (how many time/value entries, value templates, bytes per value template, etc.). It contains the following options and settings, which are relevant to calendar and scheduler functionality of the device:

- **Enable Calendar Object:** This checkbox enables a LONMARK compliant calendar object on the device. It is automatically enabled together with local schedulers, since the two are always used together.
- **Enable Scheduler Objects:** This checkbox enables local LONMARK compliant scheduler objects on the device. Checking this box will automatically enable the calendar as well.
- **Enable Remote AST Objects:** This checkbox enables the functional object for NVs, which are used to access remote AST objects. If this box is checked, the *Clients* functional block is included in the static interface.
- **Enable AST v2:** This checkbox enables the AST interface version 2 for local CEA-709 schedulers on the device. This interface is not compatible with older devices. The new interface provides access to the value label descriptions in schedule presets for remote schedulers.
- **Number of calendar patterns:** Specifies the maximum number of different exception schedules (day classes like holiday, maintenance day) supported by this calendar object.
- **Total number of date entries:** Specifies the maximum number of date definitions which may be stored by the calendar. This is the sum of all date definitions from all calendar entries. A date definition is for example a single date, a date range, or a week and day pattern.
- **Number of local schedulers:** This is the number of local scheduler objects which should be available on the device. Each local scheduler data point created in the data point manager will connect to one of these scheduler objects. There may be more scheduler objects available on the device than are actually used at a certain time. It is a good idea to have some spare scheduler objects ready, in case another scheduler is needed.

- **Number of daily schedules:** This is the maximum number of schedules supported by each scheduler object. This number must at least be 7, since a scheduler always needs to provide one schedule for each day of the week (default weekly schedule). For each special day defined by the calendar or embedded exception day, an additional daily schedule is required to support it.
- **Entries in Time/Value table:** This is the total number of entries in each scheduler defining a value template that should apply on a specific day starting at a specific time (the time table).
- **Number of value templates:** This is the maximum number of value templates supported by each scheduler.
- **Data size per value template:** This specifies the buffer size reserved to hold the data for each value template. More data points or bigger data structures require a bigger value buffer.
- **Max. number of data point maps:** Specifies the maximum number of individual data points that this scheduler is able to control.
- **AST Configuration Size:** This number in Bytes is calculated from the scheduler settings above and represents the total size of the LONMARK configuration properties file stored on the device. While certain settings can be freely edited within the given limits, the resulting configuration size is also limited.

Project Settings

General | Datapoint Naming Rules | CEA709 | CEA709 AST | Device Configuration

Calendar / Schedule Object Settings

Resources required by the current project:

Alarm server:	Yes
Local calendar:	No
Calendar patterns:	0
Total date entries:	0
Local schedulers:	0
Daily schedules:	0
Time/Value entries:	0
Value templates:	0
Total value size:	0 bytes
Datapoint maps:	0

Remote AST Objects: No

Enable Calendar Object ☐

Enable Scheduler Objects ☐

Enable Remote AST Objects ☐

Enable AST v2 ☐

Enable Alarm Server ☒

Calendar Configuration

Number of calendar patterns: 5 (max. 25)

Total number of date entries: 100 (max. 500)

Scheduler Configuration

Number of local schedulers: 10 (max. 100)

Number of daily schedules: 62 (max. 256)

Entries in Time/Value table: 128 (max. 500)

Number of value templates: 8 (max. 255)

Data size per value template: 8 (max. 32)

Max. number of data point maps: 16 (max. 64)

AST Configuration Size: 0 Byte (max. 393,216 Byte)

Auto-Set Set Defaults

Figure 59: CEA-709 AST Project Settings.

As can be seen from the above list, it is not easy to configure a LONMARK scheduler object. There are many technical parameters which need to be set and which require some knowledge of how these scheduler objects work internally. Therefore, the configuration software provides the following mechanisms to help in choosing the right settings:

- **Resources required by the current project:** The absolute minimum settings required by the current project are shown in a table at the left side of the window. This data may be used to fill in the values at the right side, but some additional resources should be planned to allow for configuration changes which need more resources.
- **Auto-Set:** This button may be used to let the configuration software decide on the best settings to use, based on the current project. Since the current projects resource usage is taken as a starting point, all schedulers and calendar patterns in the project should first be configured before this button is used.

- **Set Defaults:** This button will choose standard values for all settings. In most cases, these settings will provide more resources than necessary.

6.3.5 Device Configuration

This tab is shown in Figure 60. It is available only with the newest firmware version and can be used to configure the device through the Configurator. In the configuration tree on the left-hand side the user can select certain groups of settings, e.g. Web server settings. The dialog displays the settings of the selected group in the dialog area. The structure is similar to the menu structure on the Web UI.

Under the port configuration tree, the user can enable or disable communication protocols on the device's ports. Enabled protocols are marked with a checkmark. Click on the checkmark and toggle it. Note, that depending on the device model communication protocols on other ports may be disabled.

The IP address settings cannot be changed in this dialog. The FTP server can not be disabled in this dialog, either. This ensures that the Configurator can maintain connection to the device.

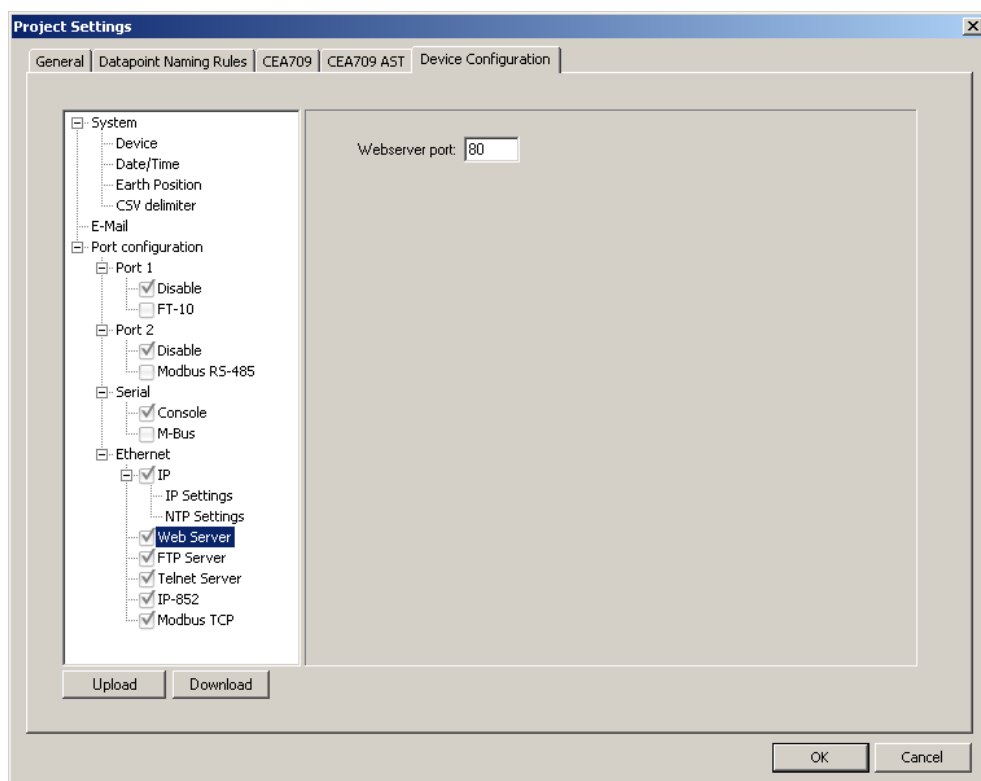


Figure 60: Device Configuration Settings

The **Upload** button can be used to get the current device settings from the device and display them in this dialog. The **Download** button can be used to explicitly transfer the settings from this dialog onto the device. Those changes will be visible immediately on the Web UI but take effect only after a reboot of the device.

6.4 Workflows for the LINX-10X

This section discusses a number of work flows for configuring the LINX-10X in different use cases in addition to the simple use case in the quick-start scenario (see Chapter 2). The description is intended to be high-level and is depicted in flow diagrams. The individual

steps refer to later sections, which describe each step in more detail. In principle, the LINX-10X Configurator supports the following use cases:

- Network Management Tool based on LNS 3.x (see Section 6.4.2)
- Non-LNS 3.x network management tool with polling (see Section 6.4.3)
- Non-LNS 3.x network management tool with bindings (see Section 6.4.4)

6.4.1 Involved Configuration Files

In the configuration process, there are a number of files involved:

- XIF file: This is the standard file format to exchange the static interface of a device. This file can be used to create a device in the database without having the LINX-10X on-line. There exists a standard XIF file for the FT port (LINX-10x_FT-10.xif) and one for the IP-852 port (LINX-10x_IP-10L.xif).
- LINX-10X Configurator project file: This file contains all ports, data points, and connections of a project. These files end with “.linx0”. It stores all relevant configuration data and is intended to be saved on a PC to backup the LINX-10X’s data point configuration.

6.4.2 Configure with LNS

The flow diagram in Figure 61 shows the steps that need to be followed in order to configure the LINX-10X in a network with LNS 3.x. In this scenario, the LINX-10X will use dynamic NVs and bindings.

First, the LINX-10X device must be added to LNS (see Section 6.5). Then the LINX-10X Configurator must be started in plug-in mode to configure the LINX-10X (see Section 6.7.1). In the Configurator, scan for the data points in the LNS database (see Section 6.7.4). Select the data points that the LINX-10X shall expose (see Section 6.7.7). Finally, the configuration needs to be downloaded to the LINX-10X (see Section 6.7.12). It is recommended to save the complete configuration to a file for being able to replace a LINX-10X in the network.

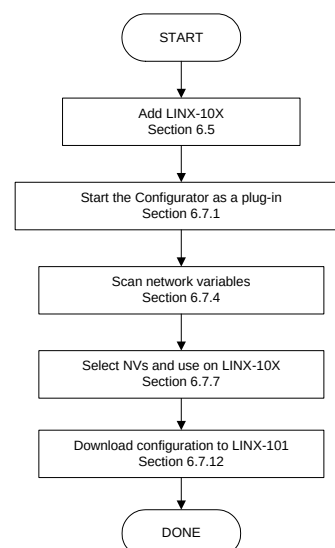


Figure 61: Basic design-flow with LNS.

To add more NVs when all bindings are in place and the LINX-10X is already being used, simply repeat the steps described above. The Configurator software will back up the bindings, create or delete the dynamic NVs, and re-create the bindings again.

6.4.3 Configure without LNS

The flow diagram in Figure 62 shows the steps that need to be followed in order to configure the LINX-10X without LNS 3.x. In this scenario the LINX-10X will use external NVs and polling. The advantage of this solution is that no bindings in the non-LNS tool (or self-binding nodes) need to be changed. This comes at the cost of a constant network load caused by polling.

Start the Configurator in stand-alone mode and connect to the LINX-10X via the FTP method (see Section 6.7.2). If changing an existing configuration, upload the current configuration from the LINX-10X (see Section 6.7.3). In the Configurator, import data points from a CSV import file (see Section 6.7.5). Select the data points that the LINX-10X shall expose (see Section 6.7.7). Alternatively, you can create external NVs manually (see Section 6.7.10). Finally, the configuration needs to be downloaded to the LINX-10X (see Section 6.7.12). It is recommended to save the complete configuration to a file for being able to replace a LINX-10X in the network.

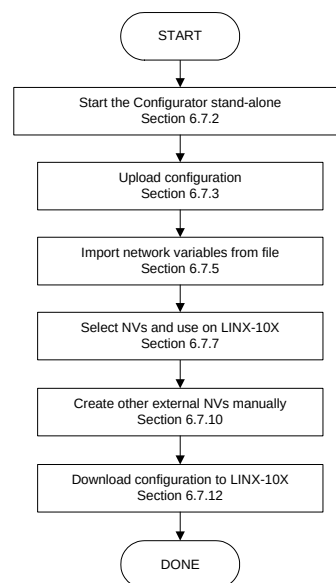


Figure 62: Basic design-flow without LNS.

6.4.4 Configure without LNS Using Bindings

The flow diagram in Figure 63 shows the steps that need to be followed in order to configure the LINX-10X without LNS 3.x. In this scenario the LINX-10X will use static NVs and bindings. The advantage of this solution is that the network load is minimized. However, the non-LNS management tool must create bindings for the LINX-10X and update an existing network.

Start the Configurator in stand-alone mode and connect to the LINX-10X via the FTP method (see Section 6.7.2). In the Configurator import data points from a CSV import file (see Section 6.7.5). Select the data points that the LINX-10X shall expose (see Section 6.7.7). For the NVs used on the LINX-10X select the “static NV” allocation type (see Section 6.7.8). Alternatively, you can create static NVs manually (see Section 6.7.9).

For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured (see Section 6.7.14). Please contact the tool’s vendor for information whether ECS is supported or not.

Download the configuration onto the LINX-10X (see Section 6.7.12). Finally, export a XIF file (see Section 0). It is recommended to save the complete configuration to a disk file for being able to replace a LINX-10X in the network.

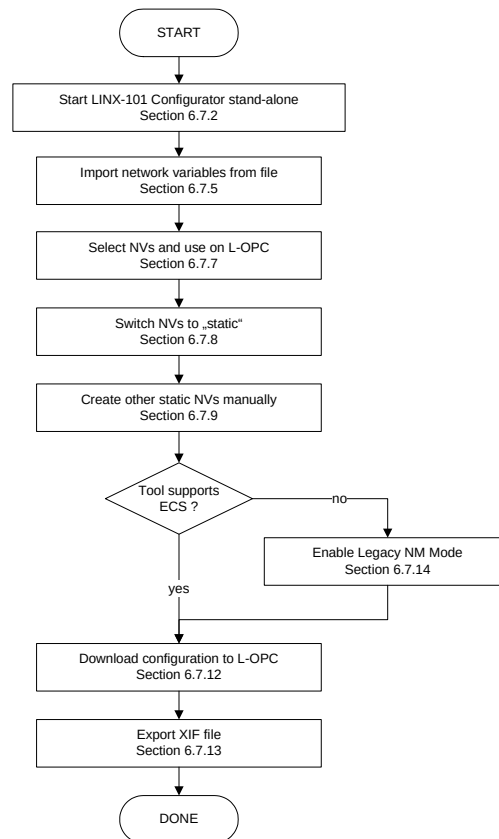


Figure 63: Basic design-flow without LNS using bindings.

To use the LINX-10X in the non-LNS management tool, commission the LINX-10X using the exported XIF file and create the bindings.

When changing a running LINX-10X configuration with existing bindings, it is recommended to create additional data points as external NVs with polling as described in Section 6.4.3. Otherwise, depending on the third-party tool, a new XIF file may be required to be exported for replacing the LINX-10X in the non-LNS tool. In this case the user would need to create all bindings again from scratch (see Section 5.5.2).

6.4.5 Replace a LINX-10X

A LINX-10X can be replaced in the network by another unit. This might be necessary if a hardware defect occurs. First of all, the replacement LINX-10X needs to be configured with the appropriate IP settings, including all relevant CEA-852 device settings. The remainder of this section focuses on the LINX-10X data point configuration. The work flow is depicted in Figure 64.

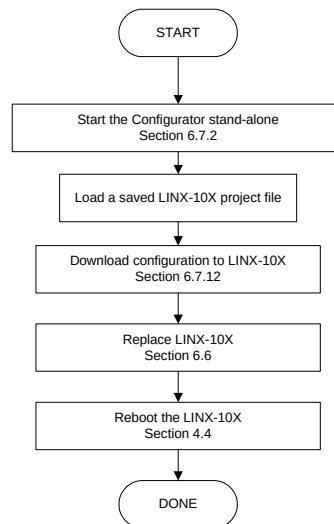


Figure 64: Basic work flow to configure a replacement device.

Start the Configurator software stand-alone and connect via the FTP method (see Section 6.7.2). Then load the LINX-10X Configurator project file from the directory, which has been saved when the original LINX-10X has been configured or modified. Double-check, if the data point configuration seems ok. Then download the configuration to the LINX-10X (see Section 6.7.12).

If using an LNS-based tool, the LINX-10X device needs to be replaced in that tool (see Section 6.6). If you are not using LNS, then refer to your network management tool's reference manual on how to replace a device. After replacing the device in the network management tool, reboot the LINX-10X (see Section 4.5).

6.5 Adding LINX-10X

To configure a LINX-10X in your LonMaker drawing, the device needs to be added to the LNS database and commissioned. This Section refers to LonMaker TE and describes how to add a LINX-10X to your database.

To Add a Device to LonMaker TE

1. In your LonMaker drawing, drag a device stencil into the drawing. Enter an appropriate name as shown in Figure 65.

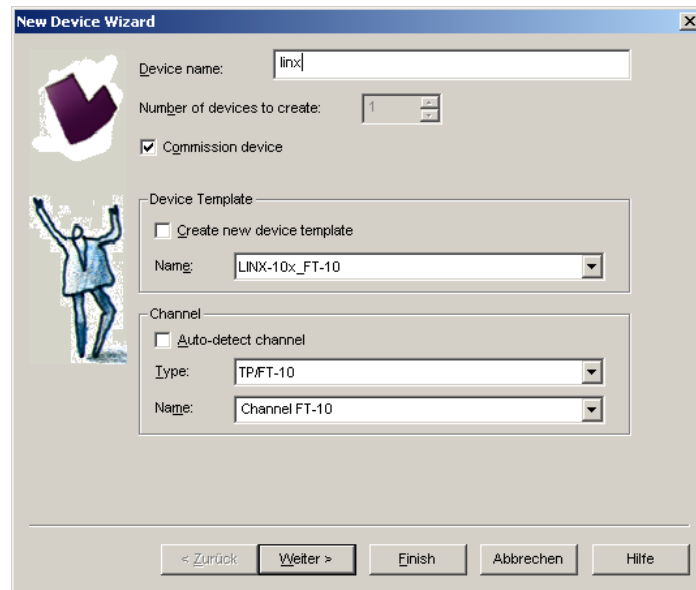


Figure 65: Create a new device in the drawing.

2. Select **Commission Device** if the LINX-10X is already connected to the network.
3. In the **Device Template** group box select the existing device template of the LINX-10X. Select “LINX-10x_FT-10”, if the LINX-10X is configured to use the FT-10 interface, or “LINX-10x_IP-10L”, if the LINX-10X is configured to be on the IP channel. For information on how to configure which port to use, refer to Section 4.2.5 for the Web UI.
4. Select the channel, which the LINX-10X is connected to and click **Next**.
5. The following dialog shown in Figure 66 appears, click **Next**.

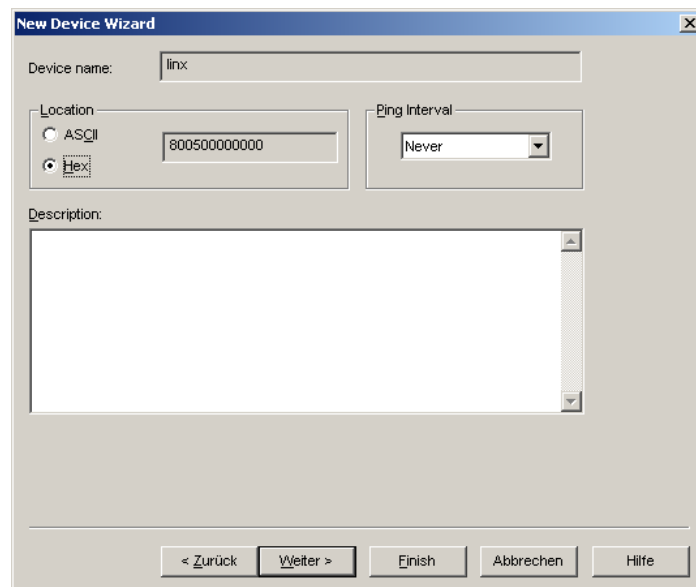


Figure 66: Leave defaults for Location.

6. Check Service Pin as the device identification method as shown in Figure 67 and click **Next**.

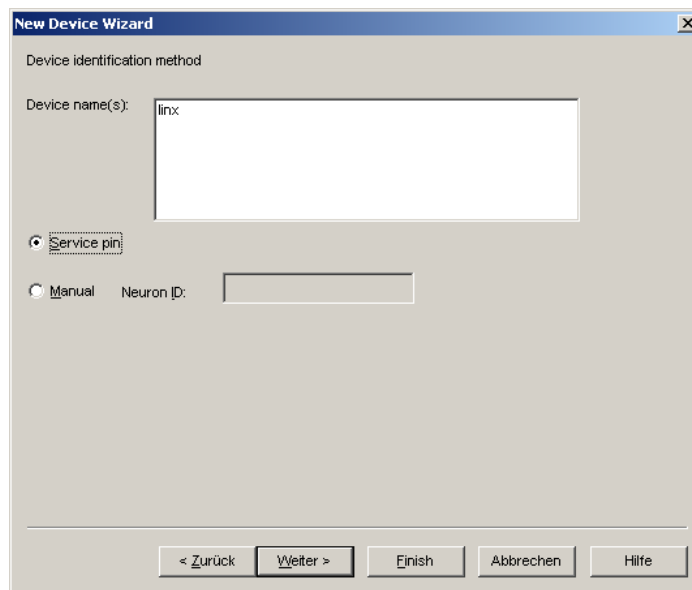


Figure 67: Use Service Pin.

7. Click **Next** in the following screens until you get to the final dialog shown in Figure 68.
8. If the device is already on-net, select **Online**.

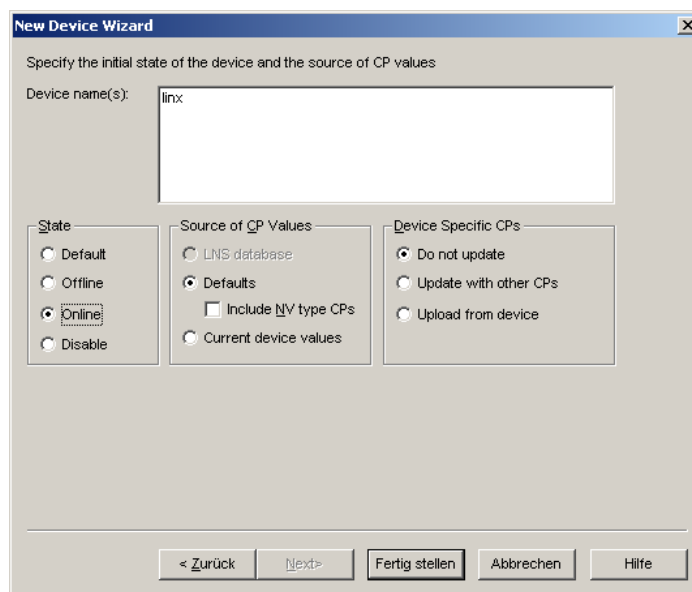
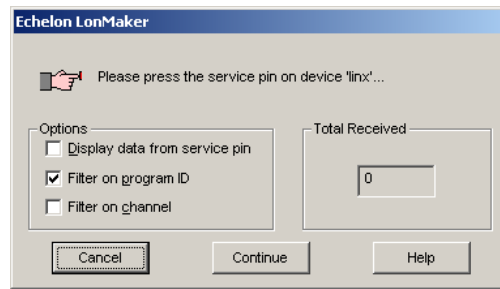


Figure 68: Final dialog.

9. Click **Finish**. A dialog will prompt to press the service pin.



10. Finally, you should get the device added to your drawing as depicted in Figure 69.

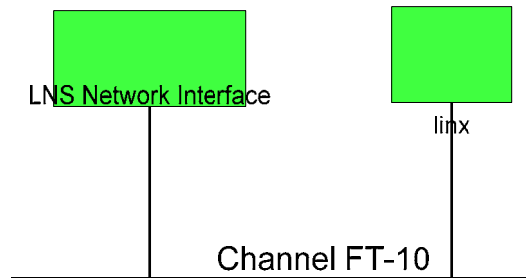


Figure 69: The LINX-10X has been added to the drawing.

6.6 Replace a LINX-10X

This Section describes how to replace as LINX-10X in your LNS database. The description refers to LonMaker TE. Let's assume there is a device 'linx' in the LNS database as shown in Figure 70.

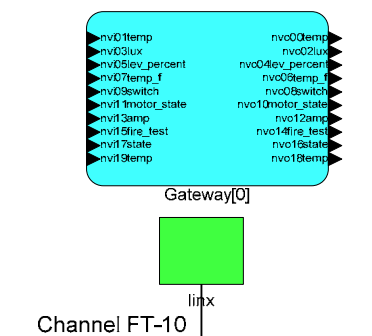


Figure 70: LonMaker drawing with one LINX-10X.

To Replace a Device in LonMaker TE

1. Select the device and right-click on the device shape.
2. Select **Commissioning** → **Replace....** This opens the LonMaker Replace Device Wizard as shown in Figure 71.

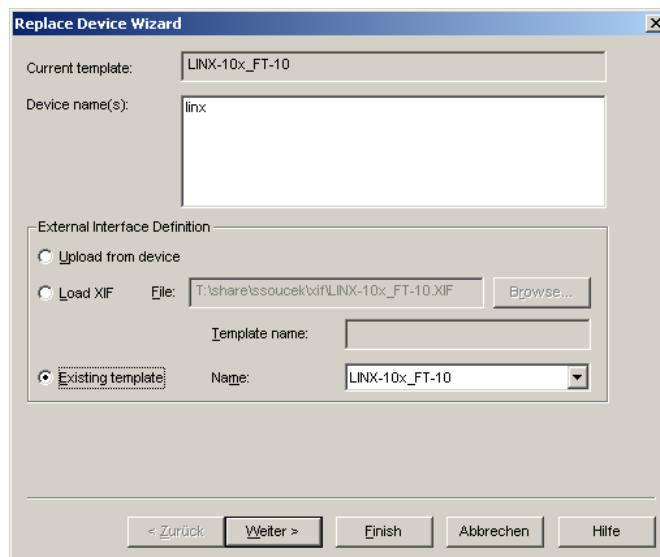


Figure 71: LonMaker replace device wizard.

3. Choose the existing device template and click **Next**.
4. In the following window shown in Figure 72 click **Next**.

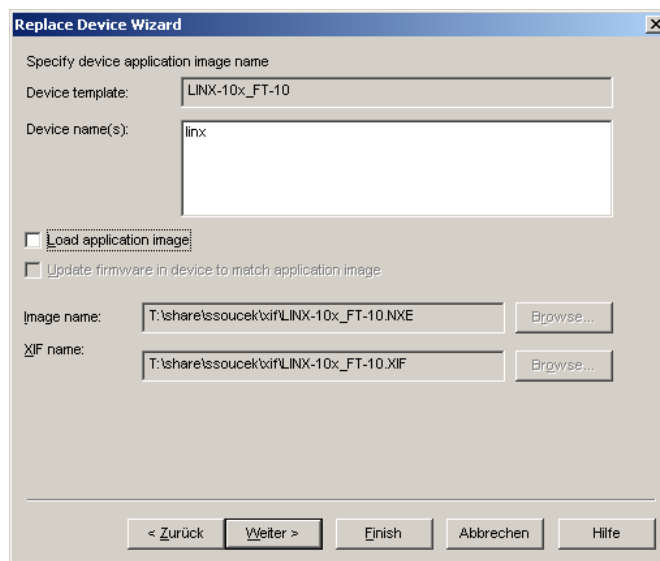


Figure 72: Click Next without loading an application image.

5. Then select **Online** as shown in Figure 73 and click **Next**.

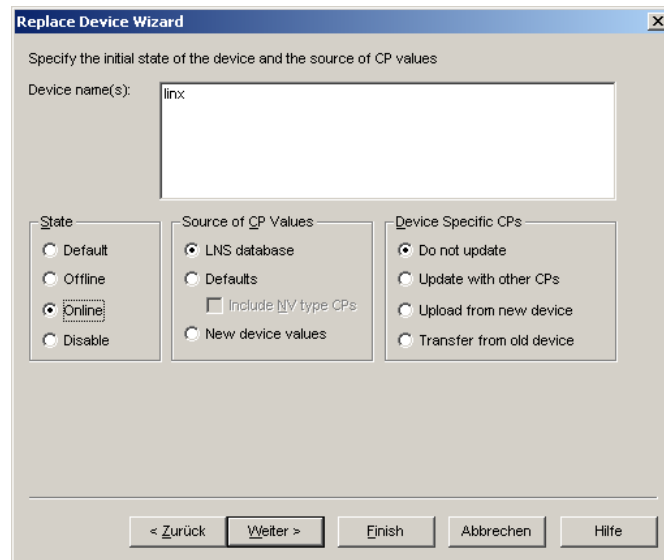


Figure 73: Select online state.

6. Select the **Service pin** method and click on **Finish** as shown in Figure 74.

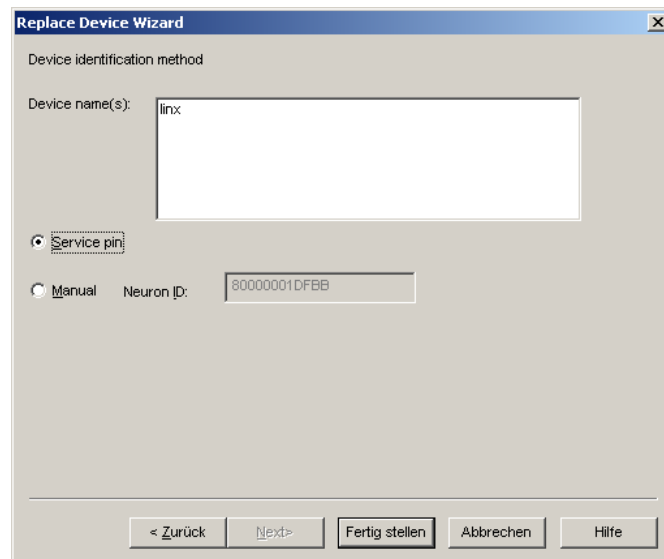
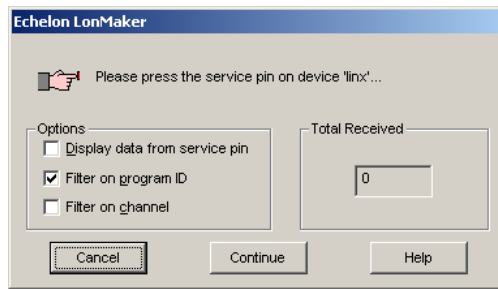


Figure 74: Select Service Pin and click Finish.

7. Then the service pin requestor opens. Press the service pin on the replacement LINX-10X on the correct port. You can also send the service pin using the Web interface (see Section 4.1).



8. After the service pin has been received, LonMaker commissions the replacement device, creates the dynamic NVs again (if any), and installs the bindings.

6.7 Using the LINX-10X Configurator

6.7.1 Starting as an LNS Plug-In

In LonMaker the plug-in is started by right-clicking on the LINX-10X device shape or the Gateway functional block and selecting **Configure...** from the pop-up window.

In NL-220, the Plug-in is started by right clicking on the LINX-10X node, then selecting the Option **LOYTEC LINX-10X Configurator** in the **PlugIns** sub menu.

In Alex, the Plug-in is started by right clicking on the LINX-10X device and selecting the **LOYTEC LINX-10X Configurator** in the **Starte PlugIn** sub menu.

A window similar to what is shown in Figure 75 should appear.

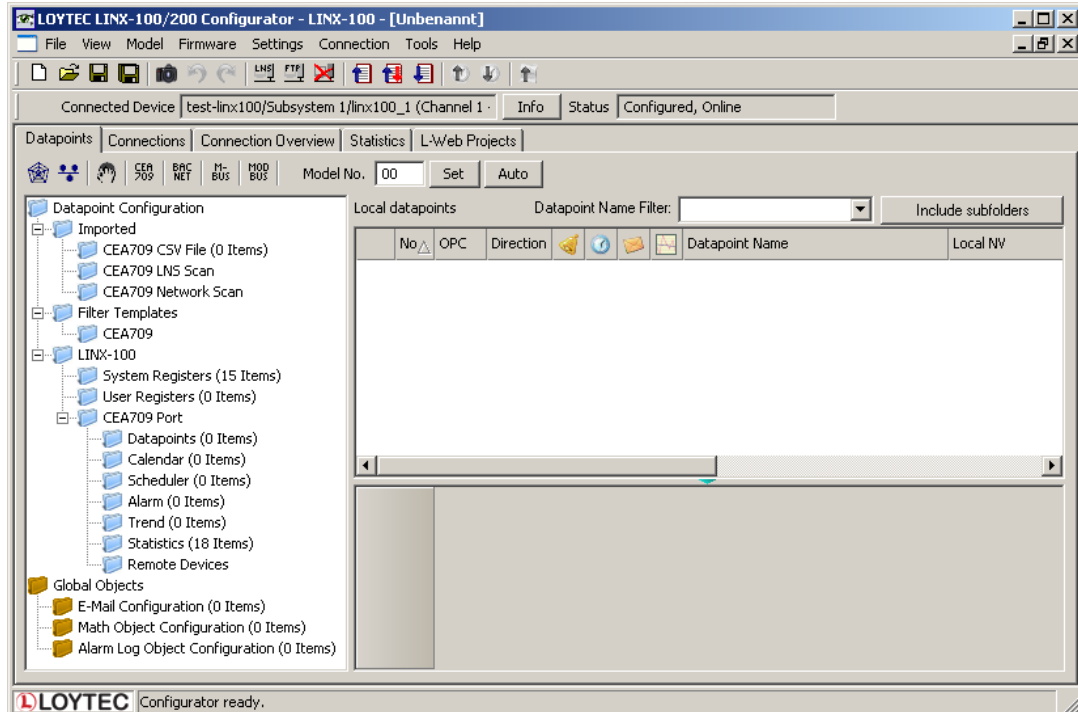


Figure 75: LINX-10X Configurator main window.

6.7.2 Starting Stand-Alone

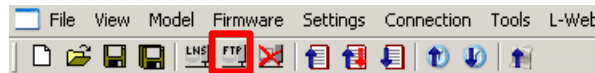
The LINX-10X can also be used without LNS-based tools. In this case, the LINX-10X Configurator needs to be started as a stand-alone application. Go to the Windows **Start**

menu, select **Programs**, **LOYTEC LINX-10X Configurator** and then click on **Configure LINX-10X**. This starts the LINX-10X Configurator and the main connections screen is displayed.

If the LINX-10X is not yet connected to the network, go to the **Firmware** menu and select the firmware version of the LINX-10X to be configured. If the LINX-10X is already connected to the network it is recommended to connect the configuration software to the LINX-10X.

To Connect to a LINX-10X Stand-Alone

1. Select the FTP connection method by clicking on the **FTP connect** button



in the tool bar of the main connections window. The FTP connect dialog as shown in Figure 76 opens.

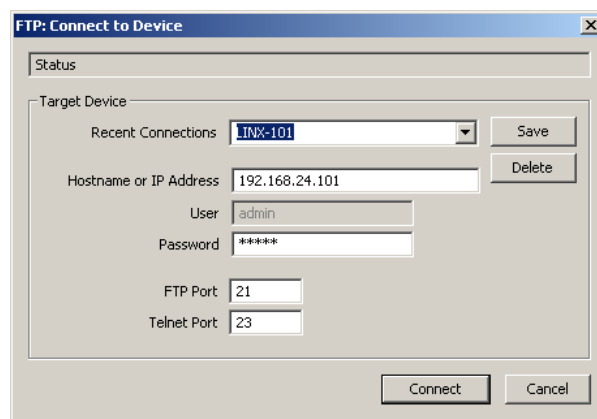


Figure 76: FTP connection dialog.

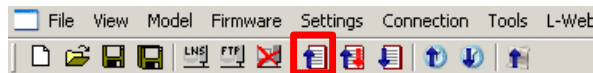
2. Enter the IP address of the LINX-10X, the user name and password. The default user is 'admin' and the default password is 'admin'.
3. Optionally, click into the **Recent Connections** field and enter a user-defined name for this connection. That name can be selected later to connect. Click on **Save** to store that connection.
4. If your device is located behind a NAT router or firewall, you may change the FTP and Telnet ports to your needs for accessing the device. Clicking **Save** also stored these settings.
5. Click on **Connect**. This establishes the connection to the device.

6.7.3 Uploading the Configuration

To get the current network variable configuration of the LINX-10X, the port interface needs to be uploaded. This will upload the entire configuration from the LINX-10X, including data points, dynamic NVs, and schedules.

To Upload a Configuration

1. Click on the **upload** button



in the tool bar. The configuration upload dialog opens up as shown in Figure 77.

2. If the check-box **Automatically sync local dynamic NVs** is marked, any manually created dynamic NVs will be uploaded and merged into the data point configuration.
3. Click on the button **Start** to start the transfer. This will upload the configuration of all ports, if the software is connected stand-alone via FTP or the network variable interface, for which the LNS plug-in was started for.

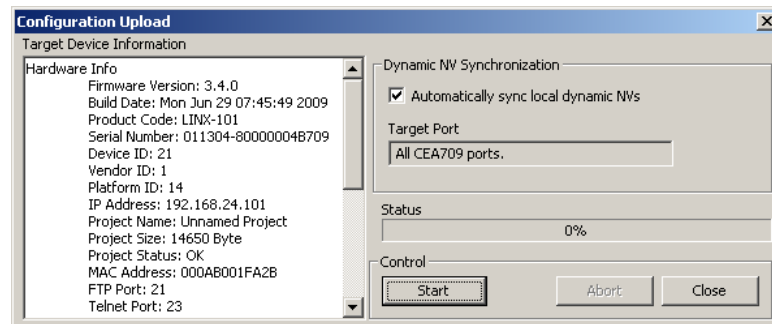


Figure 77: Configuration upload dialog.

4. When asked, if schedules shall be uploaded also, click **Yes**, if you want the current schedule configuration be extracted from the device. Note, that when doing so, the original schedules in the project are replaced by the uploaded schedules.
5. If dynamic NVs were synchronized, click on **Finish**.

6.7.4 Scanning for Network Variables

When the LINX-10X Configurator is connected to an LNS database, network variables can be scanned from that data base.

To scan network variables from the LNS database

1. Click on the **Datapoints** tab.



2. Click on the button  **Scan channel**. This scans in all NVs on all devices connected to the CEA-709 channel of the LINX-10X.
3. After the scan has completed, the folder **LNS Database Scan** is populated with the found NVs. Data point names for those NVs are automatically generated, following the data point naming rules defined in the project settings (see Section 6.3.2). By default the name is generated from node name, object name, and NV name. These names are ensured to be unique by adding a counter for multiple occurrences of the same name.

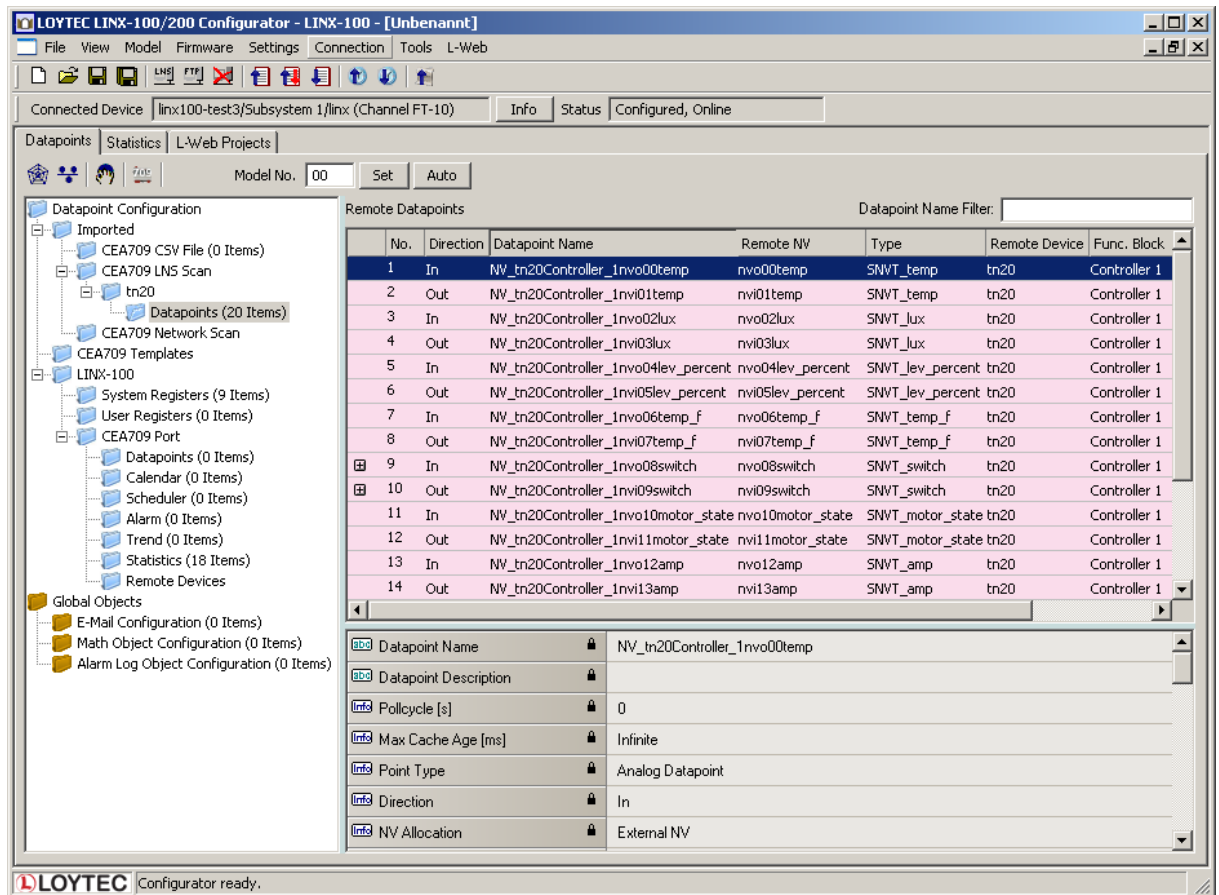


Figure 78: Scanned NVs in the LNS Database Scan Folder.

Figure 78 shows an example result of the database scan. The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

6.7.5 Importing Network Variables

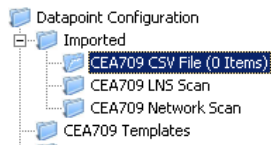
Without LNS, the tool cannot connect to an LNS database, where it scans for network variables (NVs). Therefore, the list of NVs to be used on LINX-10X has to be available in a CSV file. This file can be produced by external software or created by hand. The CSV format for importing NVs is defined in 12.2.1.

To Import NVs from a File

1. Click on the **Datapoints** tab.



2. Select the folder **CEA709 CSV File**



3. Right-click and select **Import File**. In the following file selector dialog, choose the CSV import file and click **OK**.

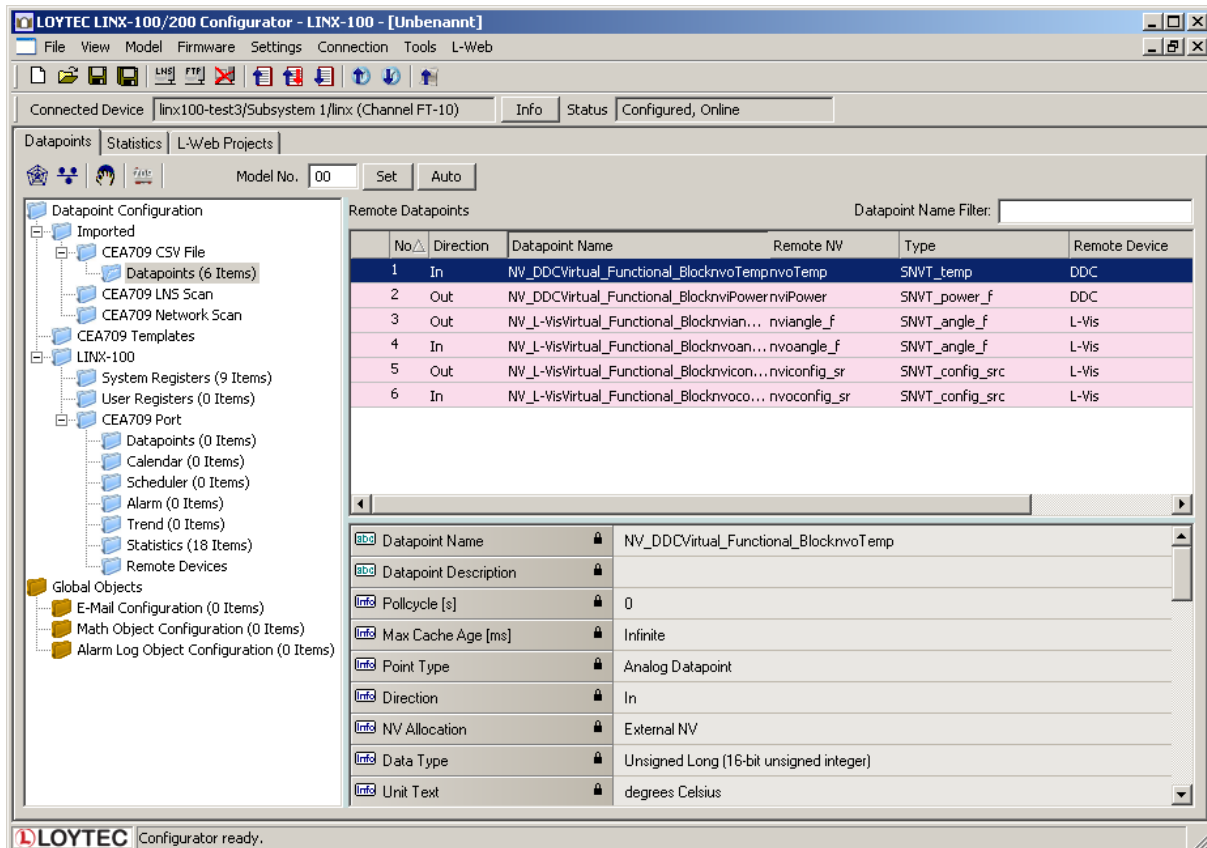


Figure 79: Imported NVs.

4. Now the CSV File folder is populated with the imported NVs as shown in Figure 79.

The list can be sorted by each column. Selecting a line will display a number of associated properties in the property view below. Multiple items can be selected by using the <Ctrl> key and clicking with the mouse. All items can be selected by pressing <Ctrl-A>.

6.7.6 Scanning NVs online from the Network

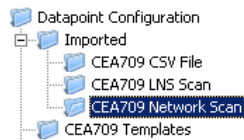
LOYTEC devices also support an online network scan on the CEA-709 network. In this scan, the device searches for other devices on the CEA-709 network and pulls in NV information of these devices. These NVs can then be used instead of importing them from a CSV file.

To scan NVs online off the CEA-709 network

1. Click on the **Datapoints** tab.



2. Select the folder **CEA709 Network Scan**.



3. Right-click on that folder and select **Scan CEA709/852 Network...**. This opens the **CEA709 Management** dialog as shown in Figure 80.

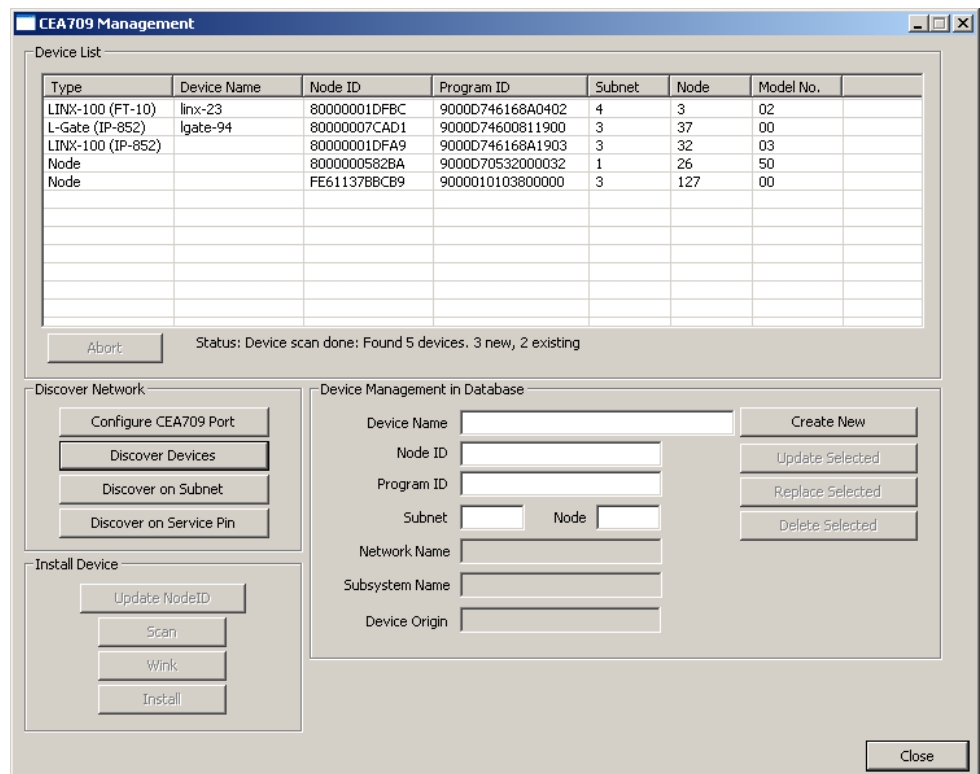


Figure 80: CEA-709 network scan dialog.

4. If the device has not been installed with a network management tool (e.g. LNS-based tool), press the **Configure CEA709 Port** button. This opens the device install dialog as shown in Figure 81.

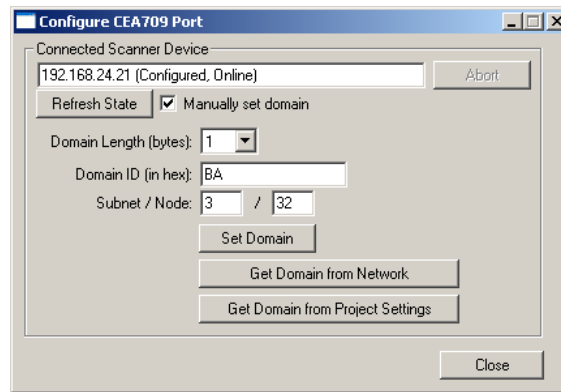


Figure 81: Configure CEA-709 port dialog.

5. Select the **Manually set domain** check-box and click the **Set** button. This sets the device configured, online to start the scan. Then click **Close**.

Note: You need to set the same domain as the devices to be scanned. Click **Get Domain from Network** and press a service pin on some other, already installed device to retrieve the domain information before setting the device online.

6. Click on the button **Discover Devices**. This starts a network scan. The results are put in the device list box.
7. Alternatively, click the button **Discover on Service Pin**. Then press the service pin of a particular device on the network. This device will be added to the device list.
8. Select a device in the device list. To give the device a usable name, enter the name in the **Device Name** field and click on the **Update Selected** button.
9. Then click the button **Scan**. This scans the NVs on the selected device and adds them to the CEA709/852 Network Scan folder as a separate sub-folder for the device as shown in Figure 82.

Tip! If you are not sure which device you have selected, click on **Wink**. The selected device will execute its wink sequence.

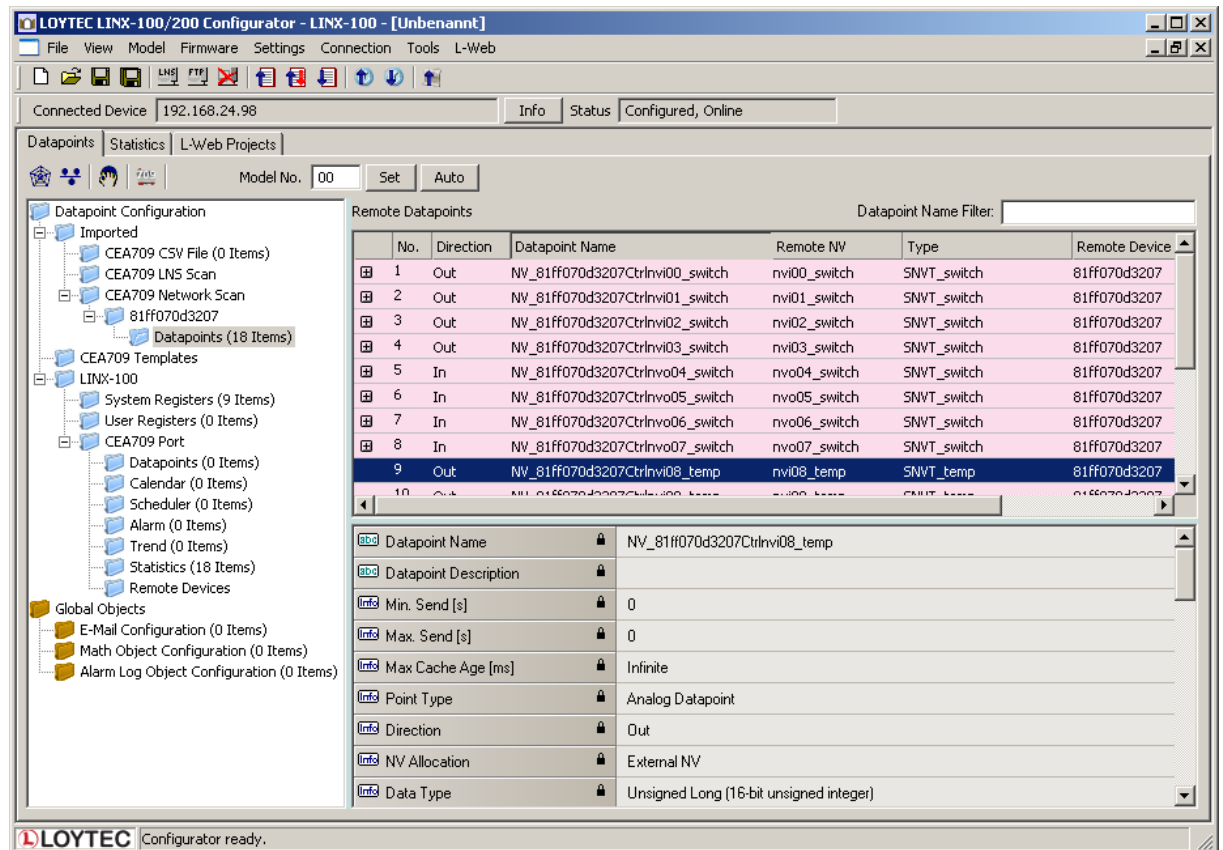


Figure 82: CEA-709 network scan results.

10. Click **Close** when all devices needed have been scanned.

6.7.7 Select and Use Network Variables

Data points in the **CEA709 LNS Scan** folder, the **CEA709 Network Scan** folder or in the **CEA709 CSV File** folder can be selected for use on the device. Select those NVs, which shall be used on the device.

To Use NVs on the Device

1. Go to any of the **CEA709 LNS Scan**, **CEA709 Network Scan** or the **CEA709 CSV File** folder.
2. Use the multi-select feature by holding the *Shift* or *Ctrl* keys pressed.
3. Click on the button  **Use on Device** in the tool bar.
4. This creates data points in the LINX-10X/CEA709 Port folder. All data points in that folder will actually be created on the LINX-10X device after downloading the configuration.

Tip!

Data points can be edited by selecting a single point or using multi-select. The available properties to be edited are displayed in the property view below.

6.7.8 Change the NV Allocation

After selecting the **Use on device** action on scanned or imported NVs, they are assigned a default NV allocation in the LINX-10X/CEA709 port folder. This default allocation can be

changed, e.g., for imported NVs when they shall be allocated as static NVs on the LINX-10X.

To Change the NV Allocation Type

1. In the data point view, select the NVs in the LINX-10X/CEA709 port folder, for which the NV allocation shall be changed.

Tip! By using *Ctrl-A* all NVs can be selected.

2. Select the **NV allocation** property as indicated by the red rectangle in Figure 83.
3. To make the data points static NVs on the LINX-10X, select **Static NV**.

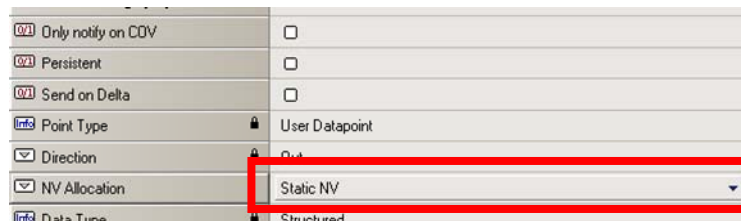


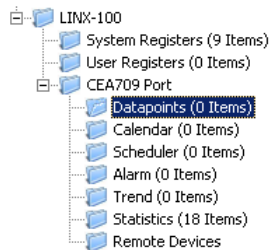
Figure 83: Change the NV allocation type.

6.7.9 Create Static NVs

The LINX-10X can be configured to change its static interface and boot with a new one. Apart from creating static NVs from scanned or imported data points, static NVs can also be created manually in the LINX-10X/CEA-709 folder.

To Create Static NVs Manually

1. Select the LINX-10X/CEA-709 Port/Datapoint folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the NV creation dialog as shown in Figure 84.

Figure 84: Create a static NV manually.

3. Enter a data point name and a programmatic name. The programmatic name is the name of the static NV which is being created.
4. Select a resource file. To create a SNVT, let the STANDARD resource file be selected.
5. Select a SNVT and a direction. If a non-standard resource file has been selected, choose from one of the UNVTs.

Tip! Recently created SNVTs are available in the **Recent NV Types** list. Click on one to set the NV type without scrolling through the drop-down box.

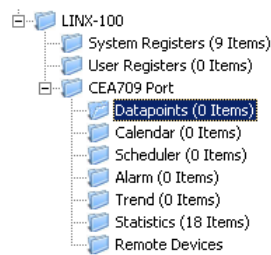
6. Choose a functional block, where this static NV shall be located in.
7. Click **Create Static NV**. The static NV is created and appears in the data point list.
8. Note, that the static interface of the LINX-10X will change as soon as static NVs are added or modified in the data point manager. This change is reflected in a new model number, which the LINX-10X will receive after the configuration download (see Section 5.5.2). Also note that the manually created static NVs are not bound automatically by the LINX-10X Configurator. They simply appear on the device and need to be bound in the network management tool.
9. Click **Close**.

6.7.10 Create External NVs

External NVs are not actually allocated NVs on the LINX-10X. Instead, the LINX-10X uses polling to read data from and explicit updates to write data to external NVs. Since external NVs do not affect the static NV interface of the LINX-10X, they can be used to extend a LINX-10X's interface configuration at run-time, where no LNS with dynamic NVs is available.

To Create an External NV manually

1. Select the LINX-10X/CEA-709 Port/Datapoints folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the NV creation dialog.
3. Click on the tab **External** as shown in Figure 85.

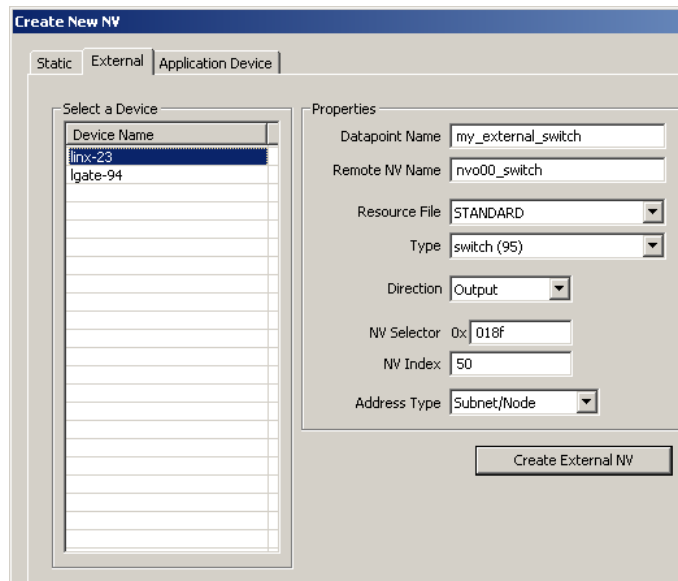


Figure 85: Create a new external NV.

4. Select the device in the box **Select a Device** on the left-hand side.
5. Enter the properties of the external NV on that device, starting with the local data point name, the remote programmatic NV name, the NV type (SNVT) and direction. Note, that the direction is the direction of the external NV on the LINX-10X. Therefore, the remote output NV nvo00_switch becomes an input on the LINX-10X. Also enter the NV selector in hexadecimal and the NV index in decimal notation. Choose the preferred addressing mode, e.g., Node ID.
6. Click **Create External NV** to add this NV to the data point list.
7. The external NV now appears in the data point list as shown in Figure 86. For external NVs which are inputs to the LINX-10X, adapt the poll cycle property to your needs.

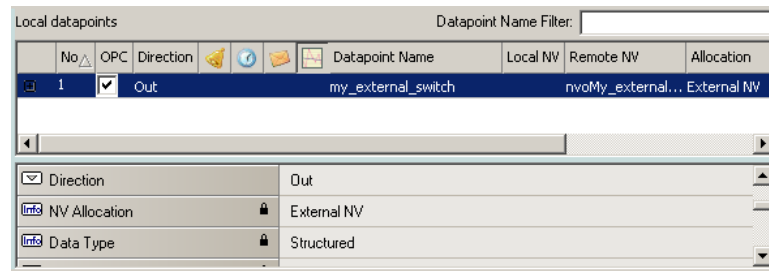


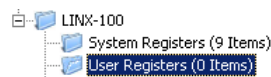
Figure 86: Manually created external NV in the port interface definition.

6.7.11 Create User Registers

User registers are data points on the device that do not have a representation on the network. Thus, they are not accessible over a specific technology. A register merely serves as a container for intermediate data (e.g., results of math objects). Since a register has no network direction, it can be written and read. Therefore, two data points are generated for each register, one for writing the register (output) and one for reading the register (input).

To Create a User Register

1. Select the LINX-10X/User Registers folder



2. Right-click in the data point list and select **New Datapoint...** in the context menu. This opens the register creation dialog as shown in Figure 87.

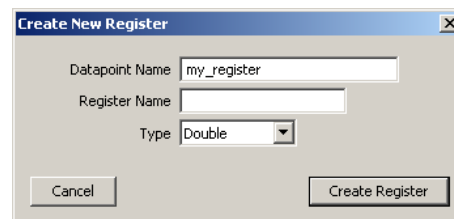


Figure 87: Create a user register.

3. Enter a **Datapoint Name** for the register. You may leave the **Register Name** blank to give the underlying register the same name as the data point.
4. Select a **Type**. Available are “Double”, “Boolean”, or “Signed Integer”.
5. Click **Create Register**.
6. Two data points now appear for the register, one for writing the register and one for reading the register as shown in Figure 88.

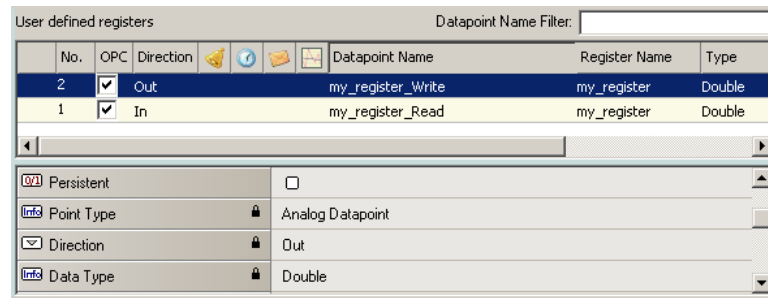


Figure 88: Manually created user register.

6.7.12 Configuration Download

After the data points have been configured, the configuration needs to be downloaded to the LINX-10X. For doing so, the LINX-10X must be online. If the LINX-10X is not yet connected to the network, the configuration can be saved to a project file on the local hard drive.

If connected via LNS, and the NVs on the LINX-10X are “Static NV” or “Dynamic NV”, the LINX-10X Configurator can create the bindings automatically. This behavior can be influenced by the download dialog. When connected via LNS, the download procedure also manages the device template upgrade in the LNS database, if the static NV interface has been changed.

To Download a Configuration

1. In the main connections window, click on the **Download Configuration** speed button



in the tool bar of the main connections window. This will open the configuration download dialog as shown in Figure 89.

2. If no bindings shall be generated, deselect the **Automatically create bindings** checkbox indicated by the red circle in Figure 89.
3. If the static NV interface has been changed, a new model number for the LINX-10X needs to be selected. This is necessary, as the static network interface of the LINX-10X changes on the CEA-709 network. The LINX-10X Configurator automatically selects a usable value, which can be overridden in the field **Model Number** marked by the blue rectangle in Figure 89.
4. Click **Start** to start the download. Each of the actions is displayed in the **Task List** section of the dialog. The current progress is indicated by the progress bar below.
5. When the download process has finished, a notification window appears, which has to be acknowledged by clicking **OK**.

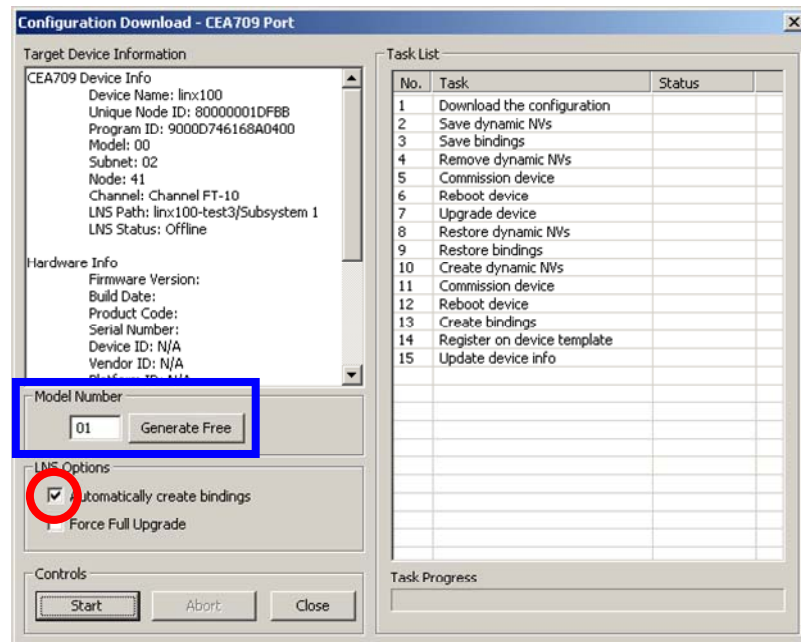


Figure 89: Configuration Download Dialog

Note, that after the download is complete, the interface changes become active on the LINX-10X (i.e., the static NV interface has changed). Refresh the network management tool to synchronize the tool with the changes to the LNS database made by the LINX-10X Configurator (e.g., use the menu “LonMaker|Refresh” in LonMaker or hit *F5* in NL-220).

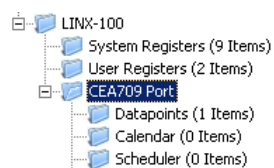
Normally, the Configurator software optimizes the download process by not executing certain LNS operations, if not necessary. For example, only those bindings and dynamic NVs are deleted and re-created, which correspond to real changes in the interface. The user can check the **Force Full Upgrade** option to clean and re-do all steps.

6.7.13 Build XIF for Port Interface

When using static NVs on the LINX-10X, the LINX-100/200 Configurator can export a new XIF file for the changed static interface

To Create a XIF File

1. Select the **CEA-709 Port** folder



2. Right-click on that folder and in the context menu select **Build XIF ...**
3. This opens a file requestor where the XIF file name needs to be entered. Select a useful name to identify the LINX-10X, e.g., as “linx-10X_1.xif”.

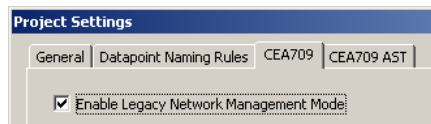
6.7.14 Enable Legacy NM Mode

For network management tools, which do not support the ECS (enhanced command set) network management commands, the legacy network management mode must be configured. Please contact the tool’s vendor for information whether ECS is supported or

not. Note, that changing to legacy network management mode changes the static interface of the device.

To Enable Legacy NM Mode

1. In the LINX-10X Configurator menu go to **Settings → Project settings ...**
2. Click on the tab **CEA709**.
3. Put a check mark in **Enable Legacy Network Management Mode**.



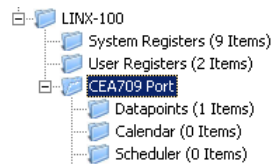
4. Click **OK**.
5. Download the configuration to activate the change.

6.7.15 Upload Dynamic NVs from Device

In LNS-based tools it is possible to create dynamic NVs on the device manually. This is a possible workflow to engineer the NV interface of the device in the LNS database. To use those manually created dynamic NVs, the LINX-10X Configurator must synchronize its dynamic NV information with the port.

To Upload Dynamic NVs

1. Select the **CEA709 Port** folder.



2. Right-click and select **Sync Dynamic NVs** in the context menu. The LINX-10X Configurator then loads any new dynamic NVs, which have been created and are not yet part of the port interface definition. The process completes when the dialog shown in Figure 90 appears.



Figure 90: Synchronizing dynamic NVs from the device.

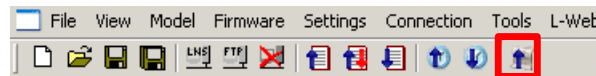
3. Click on **Finish**. The new dynamic NVs now appear in the data point list and can be edited and used on the device.

6.7.16 Upload the System Log

The system log on the device contains important log messages. Log messages are generated for important operational states (e.g., last boot time, last shutdown reason) or errors at run-time. This file is important for trouble-shooting and is available on the Web UI (see Section 4.3.5). The file can also be uploaded from the device with the LINX-10X Configurator.

To Upload the System Log

1. Connect to the LINX-10X via the FTP or LNS method (see Section 6.7.2).
2. Click on the **Upload system log** button



in the tool bar. The upload system log dialog as shown in Figure 91 opens showing the upload progress.

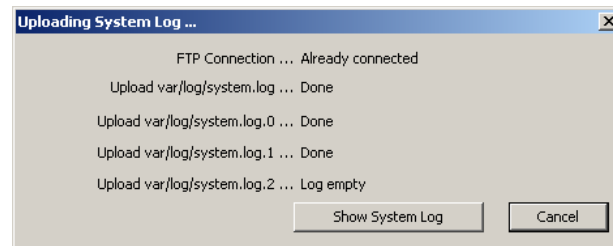


Figure 91: Upload system log dialog.

3. When the upload is finished, click on **Show System Log**. The system log window appears as shown in Figure 92.

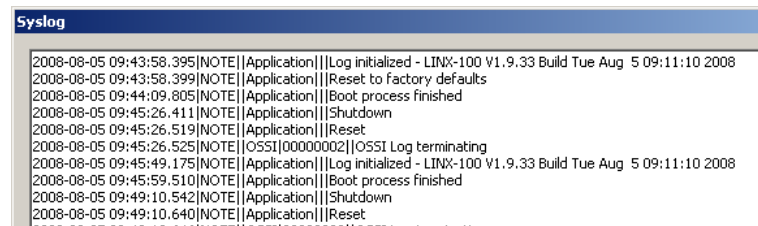


Figure 92: System log window.

4. Click on **Save** to store the system log into a file on your local hard drive.

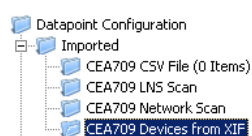
6.8 Advanced CEA-709 Configuration

6.8.1 Import Devices from XIF Templates

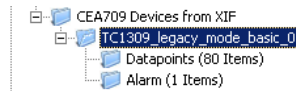
When working entirely without LNS, nodes on the network can be engineered via importing device templates from a XIF file. The Configurator provides a XIF device template import feature. Having devices imported from a XIF file is similar to have devices scanned online from the CEA-709 network, only their actual node IDs are unknown.

To Import from a XIF Template

1. Select the folder **CEA709 Devices from XIF**.



- Right-click on the folder and select **Create device(s) from XIF file...** from the context menu.
- In the file open dialog select a XIF file to import and click **Ok**.
- The imported data points appear as a device sub-folder of the **CEA709 Devices from XIF** folder named after the XIF file name.



- In that folder select those data points, which shall be used on the device and use them on the device as described in Section 6.7.7.
- Repeat the import of XIF files for as many nodes as needed. The same XIF can be imported more than one time, resulting in multiple nodes of the same type in the **CEA709 Devices from XIF** folder.

6.8.2 Install Unconfigured Devices

CEA-709 devices must be installed by a network management tool (e.g., LNS-based tool) to be available for communication. Devices can be imported from a CEA-709 network scan or from a XIF file. If no network management tool is available, the CEA-709 device manager must be used to install the unconfigured devices. To install a device the following steps need to be done:

- The imported devices must be assigned to actual devices on the network. This is done by setting a node ID that corresponds to a node on the network.
- The domain information must be written to the device and it must be set configured, online to be ready for data communication.

To Install Devices

- Open the CEA-709 management dialog by clicking on the **Manage CEA-709 Devices** speed button.



- If devices have been imported via a XIF file, they do not have a node ID (all zero). To assign the physical node to the device, select the imported device.

Node	tn50	8000000582BA	9000D70532000032	1	26	50
Node	FE611378BCB9	9000010103800000		3	127	00
LINX-100 (FT-10)	TC1309_legacy...	00000000000000	9000D746168A0401	0	0	01

- Click the **Update NodeID** button and press the service button on the network node. The node ID will be filled in to the selected device. Alternatively the node ID can also be entered manually.
- After node IDs have been assigned to all unassigned devices, select the device(s) to install in the **Device List** of the CEA-709 management dialog. Multi-select of devices is possible.
- Click the **Install** button. This opens the **Install Devices** dialog as shown in Figure 93.

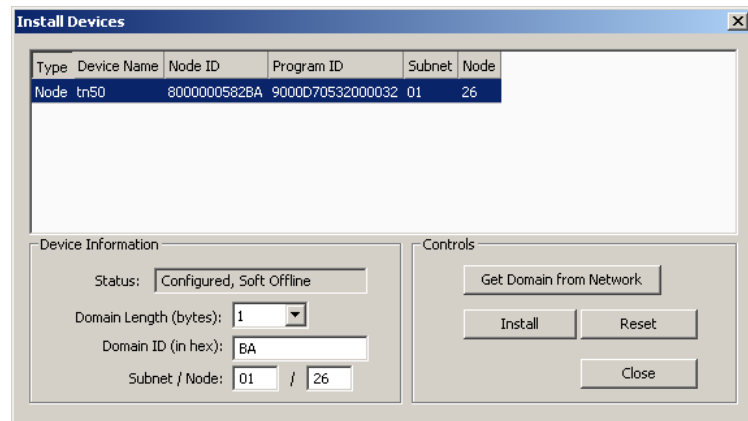


Figure 93: Install devices dialog.

6. Select the device to be installed.
7. Enter the domain information or click **Get Domain from Network** and press a service pin.
8. Enter a subnet and node address and click **Install**.
9. Some nodes won't be operable on the new settings until they are reset. Click the **Reset** button to reset the selected node.
10. Repeat this step for other unconfigured devices on the network.

6.8.3 Using Feedback Data Points

Feedback data points allow reading back the value written out over an output data point. In LONMARK systems getting a feedback value is normally accomplished by creating a dedicated feedback NV on the device, which can be bound back to the devices that are interested in the currently active value on an output.

Some nodes, however, do not possess such feedback NVs for certain functions. To support getting feedback values on such nodes, the Configurator can create feedback data points based on existing output data points. This is especially interesting for bound output NVs (static and dynamic alike). The corresponding feedback data point is an input, which uses the original output NV for polling the target NV. Once the binding is changed the new target is polled. No additional input NV needs to be created for the feedback value, if the feedback data point feature is used.

To Create a Feedback Data Point

1. Select an output data point in the data point list of the CEA-709 port folder, e.g. 'nvoHumid101'.
2. Right-click and choose Create Feedback-Point from the context menu.
3. A new input data point is created, having '_fb' appended to the original name, e.g., 'nvoHumid101_fb'. Note, that the feedback data point maps to the same NV index as the original output data point.
4. Choose an appropriate poll cycle in the data point properties for the feedback data point.

6.8.4 Working with Configuration Properties

Configuration properties (CPs) are supported by the LNS network scan and the online network scan. They can be selected and used on the device in a similar way as NVs. There is a notable difference to NVs: CPs are part of files on the remote nodes. Reading and writing CPs on the LINX-10X results in a file transfer.

The LINX-10X supports both, the LONMARK file transfer and the simpler direct memory read/write method. In both cases however, one has to keep in mind that a file transfer incurs more overhead than a simple NV read/write. Therefore, polling CPs should be done at a much slower rate than polling NVs.

Another aspect is how CPs are handled by network management tools. Formerly, those tools were the only instance that could modify CPs in devices. Therefore, most tools do not automatically read back CPs from the devices when browsing them. This can result in inconsistencies between the actual CP contents on the device and their copy in the network management tool. It is recommended to synchronize the CPs from the device into the LNS database before editing and writing them back.

To Synchronize CPs in NL220

1. Double-click on the device object in the device tree
2. Press the **Upload** button on the Configuration tab of the device properties (see Figure 94).

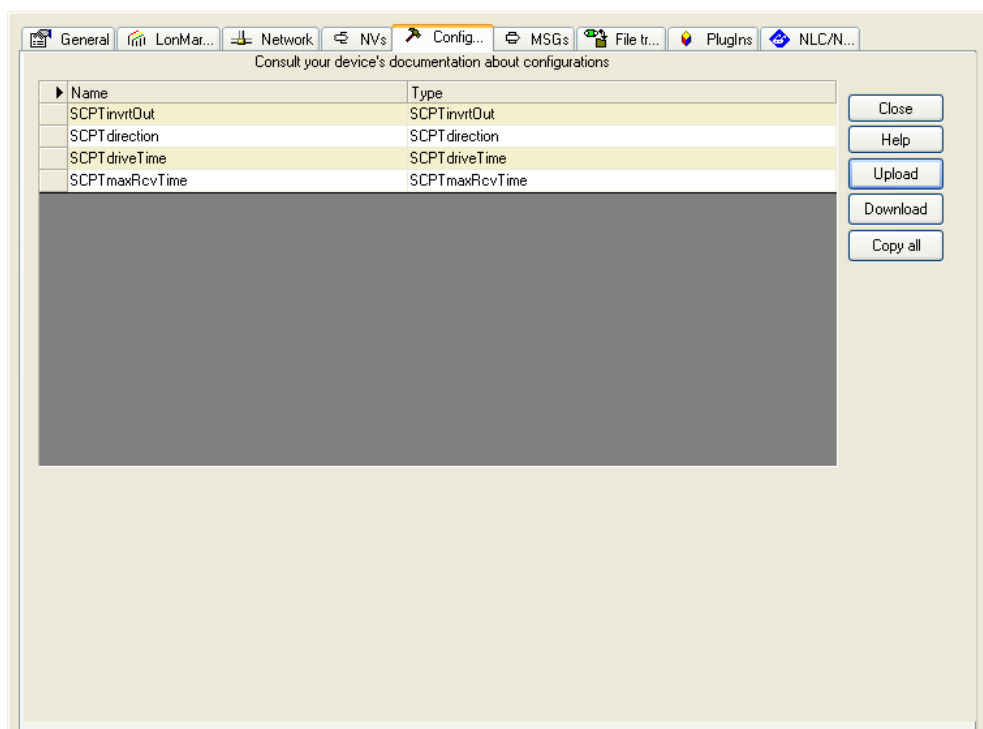


Figure 94: Configuration Tab for Configuration Properties in NL220.

To Synchronize CPs in LonMaker TE

1. Right-click on a device object and select **Commissioning → Resync CPs...** from the context menu.
2. This opens the dialog shown in Figure 95.

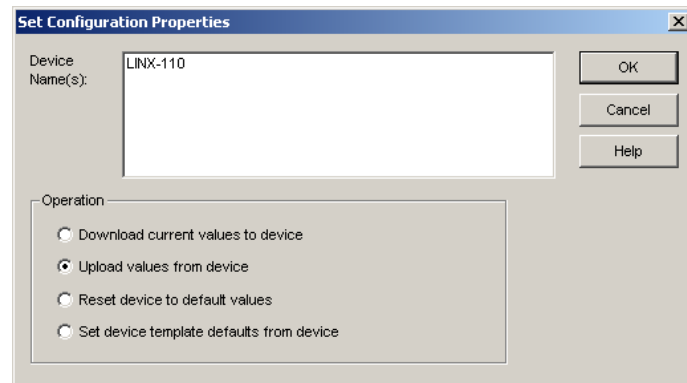


Figure 95: Set Configuration Properties in LonMaker TE.

3. In this dialog select the radio button **Upload values from device** in the **Operation** group box. To use the current settings of the device as default values for new devices, select **Set device template defaults from device**.
4. Execute the operation by clicking the **OK** button.

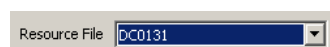
6.8.5 Working with UNVTs, UCPTs

This device supports user-defined type, including user-defined network variable types (UNVTs) and user-defined configuration property types (UCPTs). In order to interpret the contents of user-defined types, the *device resource files* supplied by the vendor must be added to the resource catalog on your PC.

Once the resource files are installed, the CEA-709 network scan and the LNS scan will display the user-defined types from the resource files. Those data points can be used on the device like regular, standard-type data points. Also manual creation of UNVTs can be performed.

To Manually Create a Static UNVT

1. Perform the steps to manually create a static NV as described in Section 6.7.9.
2. When the **Create New NV** dialog appears, change the resource file from 'STANDARD' in the **Resource File** drop-down box to the desired, user-defined resource file



3. Then select the desired UNVT from the **Type** drop-down list below. This list will display the types of the selected resource file only.
4. Click **Create Static NV** to create the UNVT on the device.

6.9 Connections

6.9.1 Create a New Connection

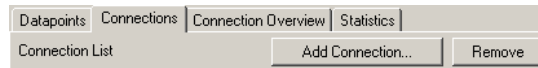
After having configured the device's network ports with data points, internal connections between those data points can be created. Usually, the manual method to create a connection is used to create connections between different named data points.

A connection is an internal mapping in the device between input and output data points. A connection always consists of *one* hub data point and *one or multiple* target data points.

Hub data points can be input or output. If the hub data point is an input, then the target data points must be output and vice versa. All data points in the connection must be of a compatible type.

To manually create a new connection

1. Click on the **Connections** tab



in the tool bar of the main connections window and press **Add Connection....** A new connection is added to the connection list. Rename the connection if you want to do so.

2. Click on **Select Hub...** to select the hub point. This opens a list of all available data points. Select one and press **OK**.
3. Then click on **Add Target...** Similar to 2) select all target data points. You may use multi-select to select more than one data point at a time.

Note: By default only compatible data points are displayed. Sometimes compatible data points are available as member points (e.g., a SNVT structure member). Click on  to expand the data point and select the desired member point.

4. Now the connection dialog contains a hub and two target data point as shown in Figure 96.

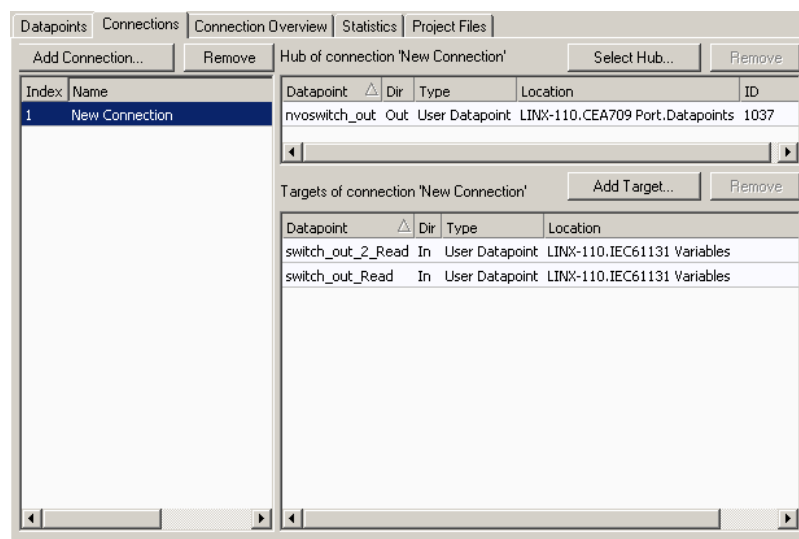


Figure 96: Connection dialog with hub and target points.

6.9.2 Create Connections from a CSV File

A quick way to perform batch edit on connections is to export and import connections from the connections CSV file. Each line in the connections CSV file identifies a connection. The first column is the connection name. The second column specifies the hub data point. The full path to the data point must be specified using the dot '.' as the folder separator. The third and following columns specify the target data points.

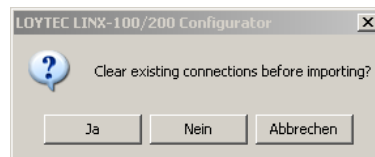
To Create Connection from a CSV File

1. Select the menu **Tools → Export Connections ...**
2. Select an appropriate file name and export.
3. Edit the connections CSV file. An example is shown in Figure 97.

```
#connection_csv_ver,1
#ConnectionName,HubDPName,TargetDPName
nvoAbs_humid1,LINX-100.CEA709          Port.abs_humid1,LINX-100.User
Registers.abs_humid1
nvoAbs_humid2,LINX-100.CEA709          Port.abs_humid2,LINX-100.User
Registers.abs_humid2
nvoAbs_humid3,LINX-100.CEA709          Port.abs_humid3,LINX-100.User
Registers.abs_humid3
nvoAbs_humid4,LINX-100.CEA709          Port.abs_humid4,LINX-100.User
Registers.abs_humid4
```

Figure 97: Example Connection CSV File.

4. Select the menu **Tools → Import Connections ...**
5. If connections that are not part of the connection CSV file shall be deleted, click **Yes** when prompted. Click **No** if the other connections shall be left as is.



6. Choose the file to import and click **Ok**.
7. When the import has completed, optionally view the log to check, which connections have been added, modified, and deleted.

6.9.3 Modify Connections

Connections can be edited and deleted. This is also done in the **Connections** tab of the main window. Editing connections does not influence the data point configuration. This means, when deleting a connection or adding/removing data points to/from a connection, the data points are not deleted.

To Edit a Connection

1. Change to the **Connections** tab of the main window.
2. Select the connection to edit. Then follow the steps as applied when creating a connection.
3. To delete a target, select the target and click on **Remove Target(s)**.

To Delete a Connection

1. Change to the **Connections** tab of the main window.
2. Select the connection for removal. Use multi-select to select more than one connection.
3. Click **Remove**.

6.9.4 Connection Overview

Select the **Connection Summary** tab to get a graphical representation of all connections. It represents the two connected data points, their technology they are based on and the direction of the connection. An example for the overview is shown in Figure 98.

Datapoints	Connections	Connection Summary		Statistics	
NV	Datapoint	Dir	Datapoint	NV	Connection
nviHumid	L-Proxy.CEA709 Port 1 (FT).humid_def	➡	L-Proxy.CEA709 Port 2 (FT).humid_def	nviHumid	nviHumid (1037)
nviHumid	L-Proxy.CEA709 Port 2 (FT).humid_def	➡	L-Proxy.CEA709 Port 1 (FT).humid_def	nviHumid	nviHumid (1037)
nviTemp	L-Proxy.CEA709 Port 1 (FT).temp_def_p...	➡	L-Proxy.CEA709 Port 2 (FT).temp_def...	nviTemp	nviTemp (1039)
nviTemp	L-Proxy.CEA709 Port 2 (FT).temp_def_p...	➡	L-Proxy.CEA709 Port 1 (FT).temp_def...	nviTemp	nviTemp (1039)
nviState1	L-Proxy.CEA709 Port 1 (FT).state1_def	➡	L-Proxy.CEA709 Port 2 (FT).state1_def	nviState1	nviState1 (104B)
nviState1	L-Proxy.CEA709 Port 2 (FT).state1_def	➡	L-Proxy.CEA709 Port 1 (FT).state1_def	nviState1	nviState1 (104B)
nviState2	L-Proxy.CEA709 Port 1 (FT).state2_def...	➡	L-Proxy.CEA709 Port 2 (FT).state2_d...	nviState2	nviState2 (105D)
nviState2	L-Proxy.CEA709 Port 2 (FT).state2_def...	➡	L-Proxy.CEA709 Port 1 (FT).state2_d...	nviState2	nviState2 (105D)
nviMotor1	L-Proxy.CEA709 Port 1 (FT).motor1_def	➡	L-Proxy.CEA709 Port 2 (FT).motor1_def	nviMotor1	nviMotor1 (105F)
nviMotor1	L-Proxy.CEA709 Port 2 (FT).motor1_def	➡	L-Proxy.CEA709 Port 1 (FT).motor1_def	nviMotor1	nviMotor1 (105F)
nviMotor2	L-Proxy.CEA709 Port 1 (FT).motor1_def...	➡	L-Proxy.CEA709 Port 2 (FT).motor1_d...	nviMotor2	nviMotor2 (1061)
nviMotor2	L-Proxy.CEA709 Port 2 (FT).motor1_def...	➡	L-Proxy.CEA709 Port 1 (FT).motor1_d...	nviMotor2	nviMotor2 (1061)

Figure 98: Connections Summary.

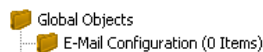
6.10 E-mail Templates

6.10.1 Create an E-mail Template

E-mail templates are used to assemble and transmit e-mails when certain trigger conditions occur. The e-mail template contains the destination e-mail address, the subject, and text. Variable parameters can be added to the text by using data point sources. The transmission of an e-mail is triggered by one or more trigger data points. For setting up e-mails, the e-mail account information has to be configured on the device, e.g., on the Web UI (see **Fehler! Verweisquelle konnte nicht gefunden werden.**).

To Create an E-mail Template

1. Under the **Global Objects** folder, select the **E-mail Configuration** sub-folder.



2. Right-click and select **New E-mail Template ...** from the context menu.
3. In the **Configure E-mail Template** dialog, which is shown in Figure 99 enter the **To** address and the **Subject**. Optionally, **Cc** and **Bcc** addresses can be specified.

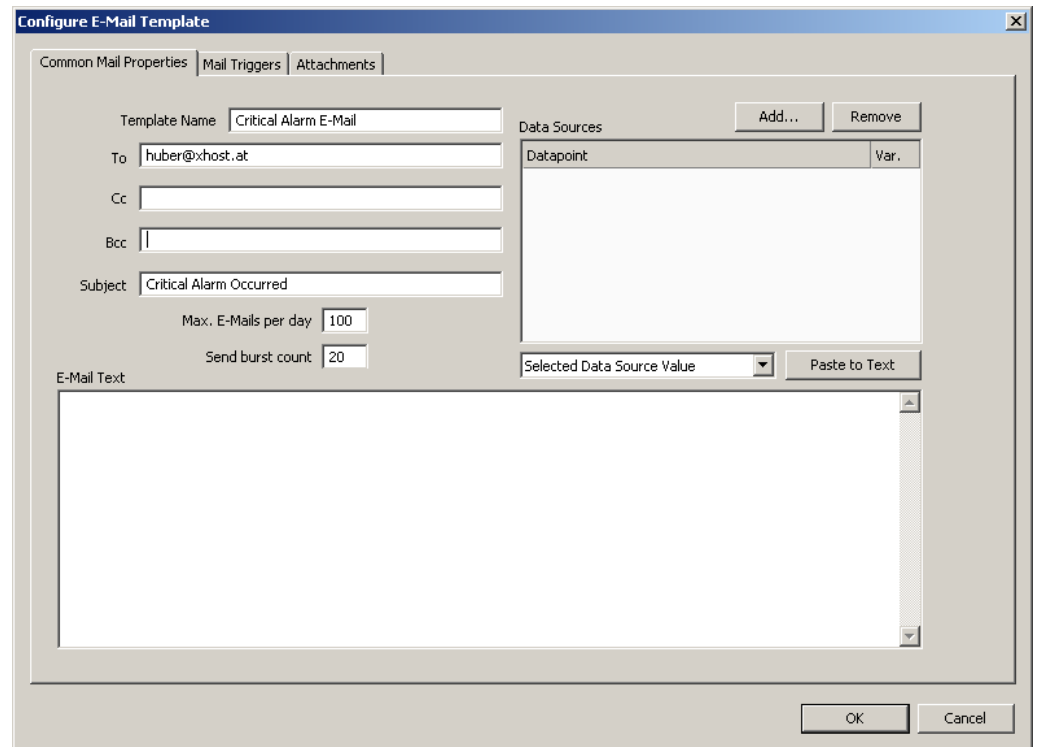
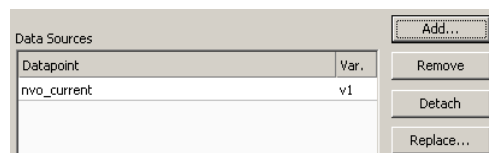
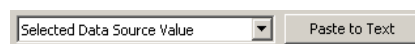


Figure 99: Configure E-Mail Template Dialog.

4. Enter text in the **E-mail Text** multi-line field.
5. If the e-mail text shall contain values of data points, add data points to the **Data Sources** list by clicking the **Add...** button.
6. A data point selector dialog opens. Select one or more data points and click **OK**. The selected data point appears in the **Data Sources** list.



7. Select the data point in the **Data Sources** list. In the drop-down box underneath select **Selected Data Source Value** and click the **Paste to Text** button.



8. A place holder **%{v1}** for the data point value appears now in the e-mail text.
9. To replace an existing data source select the data point in the **Data Sources** list and click the **Replace ...** button. This opens a data point selector dialog for choosing the replacement data point.

6.10.2 Trigger E-mails

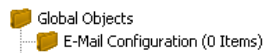
E-mail templates are used to assemble and transmit e-mails when certain trigger conditions occur. For an e-mail template, one or more trigger conditions can be defined. The e-mail will be sent, when one of the trigger conditions is activated. Depending of the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

The trigger for sending an e-mail can be enabled or disabled altogether by using an *enable* data point. This data point must be of type *binary*. If the value of that enable data point is TRUE, the trigger conditions are evaluated. If the value of the enable is FALSE, no e-mails are be triggered.

To Create an E-mail Trigger

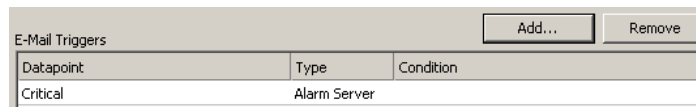
1. Under the **Global Objects** folder, select the **E-mail Configuration** sub-folder.



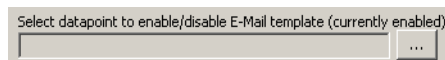
2. Right-click and select **Configure E-mail Template ...** from the context menu.
3. Change to the **Mail Triggers** tab.

Note: Of course, you can also change directly to the **Mail Triggers** tab when creating an e-mail template.

4. Click the **Add...** button. A data point selection dialog opens.
5. Select one or more data points and click **OK**.
6. The triggers appear now in the **Mail Triggers** list. The data points that serve as e-mail triggers also appear with the e-mail icon  in the data point list.



7. In the **Manage Trigger Conditions** you can setup the trigger condition depending on the trigger data point class.
8. If the trigger condition is depending on the value of an enabling data point, you can add an enable data point by clicking on the  button.



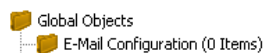
9. To remove such a trigger enable, click the **Remove Enable Trigger** button.

6.10.3 Attachments

E-mail templates can be configured to have file attachments. Basically, any file of the device can be specified as an attachment.

To Configure Attachments

1. Under the **Global Objects** folder, select the **E-mail Configuration** sub-folder.



2. Right-click and select **Configure E-mail Template ...** from the context menu.

3. Change to the **Attachments** tab.

Note: Of course, you can also change directly to the **Attachments** tab when creating an e-mail template.

4. Select an available file from the **Attach File** drop-down box.



5. Click the **Add** button. The file appears in the **Attachments** list.

Attachment	Device File Path
system.log	/var/log/system.log

6. To remove an attachment, select the attachment file in the **Attachments** list and click the button **Remove**.

6.10.4 Limit E-mail Send Rate

The transmission of e-mails is triggered by the configured trigger conditions. It is not predictable, how often the trigger condition will cause the transmission of an e-mail. The e-mail template can be configured to limit the number of transmitted e-mails. This is done in the Configure E-mail Template dialog.

To configure an E-mail Rate Limit, configure the settings:

- **Max. E-mails per day:** This setting defines how many e-mails can be sent on average per day. The actual number of transmitted e-mails on a specific day may be slightly higher than this setting, depending on burst rates. The default is 100 e-mails per day. This results in an average interval of one e-mail per 14 minutes.
- **Send burst count:** This setting defines how many e-mails may be transmitted shortly after each other not limited by the above average interval. After the burst count, the average mails per day limit takes effect. The default is a maximum of 20 e-mails in a row.

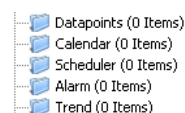
6.11 Local Schedule and Calendar

6.11.1 Create a local Calendar

As the first step, the required data points must be created. A calendar must be created, if the schedules shall work with exception days, such as “Holidays”. If it suffices for schedules to define daily schedules for normal weekdays only, no calendar needs to be created.

To Create a local Calendar

1. Under the port folder, select the **Calendar** sub-folder to create a calendar.



2. Right-click in the data point list view and select **New local Calendar ...**
3. In the Create New Calendar dialog box (as shown in Figure 100) enter Name and Description of the calendar. Correct the effective period if necessary.

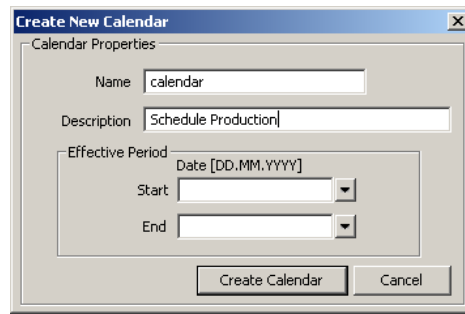


Figure 100: Create New Calendar dialog box.

4. Click **Create Calendar**. The calendar appears now in the data point list view.

6.11.2 Create Calendar Pattern

When a local calendar is used, it needs to be configured with calendar patterns. A calendar pattern represents a class of days such as “Holidays”. The calendar patterns can then be used in a schedule to define daily schedules for exception days. The available calendar patterns should be created when the system configuration is engineered. The actually dates in the calendar patterns can be modified later at run-time.

To Create a Calendar Pattern

1. Select an existing calendar data point.
2. Right-click and select **Create Calendar Pattern...**
3. Enter a Pattern Name in the **Create Calendar Pattern** dialog



4. Click **Create Pattern**. The dialog closes and the calendar pattern appears beneath the calendar data point.

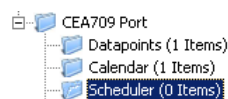
Local calendar objects						
	No.	Direction	Calendar Name	Index	Func. Block	Use ID
	1	In	calendar			1030
	1.1		Holidays			1032

6.11.3 Create a Local Scheduler

For scheduling data points, a scheduler object must be created. Under each port folder, multiple local scheduler objects can be created. These local schedulers can then be configured to schedule data points.

To Create a Local Scheduler

1. Under the port folder, select the Scheduler sub-folder to create a scheduler.



2. Right-click in the data point list view and select **New Local Scheduler ...**.
3. Enter a name for the schedule and a description. Note, that the schedule automatically detects a calendar, if it has previously been created.

- Click **Create Schedule**. The new schedule appears in the data point list of the Scheduler sub-folder.

6.11.4 Configure Scheduled Data Points

When a local scheduler has been created, it needs to be configured, which data points it shall schedule. This is done by attaching data points to the scheduler. Note, that there may be limits, how many and which data points may be attached (see Section 6.11.11).

This configuration must be done as an initial setup. Which data points are scheduled cannot be changed at run-time. The daily schedules, however, can be changed later in the Web UI or over the network.

To Attach Data Points to a Scheduler

- Select the scheduler data point in the Scheduler sub-folder.
- Right-click and select **Configure Schedule** from the context menu. The same dialog which appears when a new scheduler is created is shown and allows configuring the scheduler. Of course, this step can also be done directly when the data point is created.
- Select the tab **Scheduled Datapoints**.

Datapoint	Description	Group	Default
-----------	-------------	-------	---------

- Click the button **Attach Datapoints**. This opens another data point selector window.
- Select the data points to attach and click **OK**. For each of the attached data points, one or more lines appear in the list below the attach button. If the attached point is a structure, there will be one line for each element of the structure.

Tip!

Data points can also be attached to a scheduler by selecting a data point in the data point manager, drag it onto a scheduler data point and drop it on the scheduler data point.

- Enter a short text in the **Description** field in the second column of each line. This text will serve as a label, which will be shown on the device's UI to identify the data point.

Datapoint	Description	Location	Group	Default
nvo_current		LINX-11...	-	0.00

- Add new value presets by entering a name and pressing the **Create** button next to the input field.



New Preset Name

Tip! To generate presets automatically for multi-state data points, click the **Auto-Create** button. This button is available, if no other presets have been defined yet.

- For each new preset, a new column will appear in the list. In this column, enter the desired value for each of the attached points, which will be set when this value template is scheduled. The user may later edit the values for each preset on the device but cannot add new value presets unless there is only one line (one value) in the list.

Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	-	0.00	21.00	16.00

- If there are multiple output values which belong together, they can be grouped in order to save space on the device. For each group, the entered value is stored only once, even if there are more data points in the same group.

Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint_2		LINX-110.CEA709 Port.Datapoints	1	0.00	21.00	16.00
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	1	0.00	21.00	16.00

- When done with the point and value setup, switch back to the **Configuration** tab or click **Save Changes** to leave the dialog.

Tip! A shortcut to creating a scheduler object and attaching a data point is to select a data point in the data point manager, right-click on it and choose **Schedule Datapoint** from the context menu. This generates a scheduler and links that data point to it.

6.11.5 Configure Daily Schedules

Once a scheduler is configured with attached data points and value presets, the daily schedules can be defined. This can be done on the device or over the network at run-time, or also in the configuration software. A daily schedule defines the time and value sequences in a 24-hour period starting at 00:00 and ending at 23:59 hours. For each weekday a daily schedule can be configured.

In addition, daily schedules can be configured for exception days from a calendar, such as "Holidays". An exception day always overrides a normal weekday. If more than one exception day is used, a priority must be assigned. This is necessary so that the system knows which schedule to follow on a day which matches more than one calendar pattern.

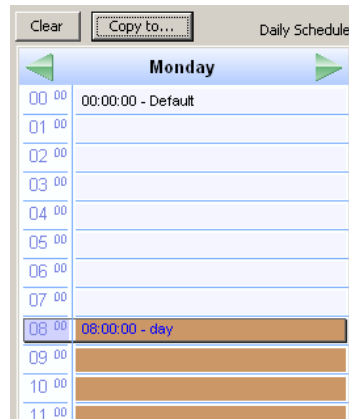
To Configure a Daily Schedule

- Open the **Configure Schedule** dialog and click on the **Configuration** tab (see Section 6.11.4).
- Select the day for which to configure a daily schedule.

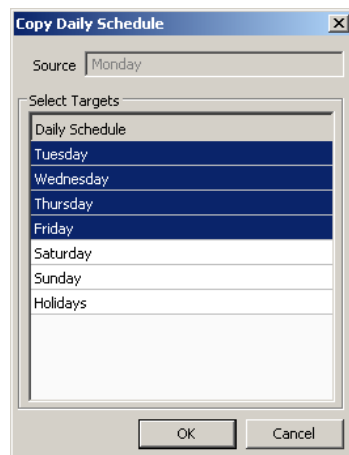
Weekly / Exception Schedule Configuration			
Weekday / Exception	Priority	Events	Use
Mon	-	0	☒
Tue	-	0	☒
Wed	-	0	☒
Thu	-	0	☒
Fri	-	0	☒
Sat	-	0	☒
Sun	-	0	☒
Holidays	1 (highest)	0	☐

- Select a value preset in the **Available Data Presets** box on the upper right-hand side.

4. Drag and drop the preset from this list into the time table area to define the desired output values on the day schedule.



5. Completed daily schedules may be copied to other days using the **Copy to** button. For example, the Monday may serve as the template for a regular work day and be copied to Tuesday till Friday. Then click **OK**.

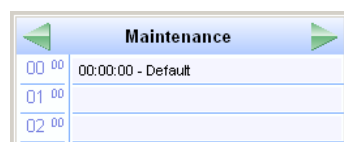


To Use Exception Days

1. Select a calendar pattern, which shall be used as an exception day and place a checkmark on it.

Sun	-	0	☒
Maintenance	2	0	☒
Holidays	1 (highest)	0	☒

2. Edit the daily schedule.



3. If more than one calendar pattern is used, edit the priorities. For example, if a given calendar day falls in both categories, "Holidays" and "Maintenance", the exception day with the higher priority becomes effective on that day. The highest available priority is marked **highest**. Note that the actual priority values depend on the technology (see Section 6.11.11).

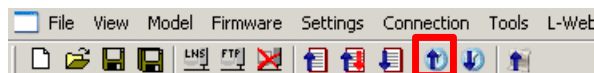
Important! *Choose different priorities for different exceptions. If two exceptions are valid for a given day and their priorities are equal, it is not determined, which exception is in effect.*

6.11.6 Configure Exception Days

When a local calendar is used, its calendar patterns need to be configured with exception days (pattern entries). The calendar patterns can be configured in the LINX-100/200 Configurator software or be modified at run-time over the Web UI or over the network. When configuring in the software, the current exception days should be uploaded from the device, to work on the current configuration.

To Configure Exception Days in a Calendar Pattern

1. Click on the **Upload calendar/scheduler configuration** button



in the tool bar of the main connections window. Click **OK** when the upload is finished.

2. Select the **Calendar** sub-folder and select the calendar pattern, which shall be configured

	No.	Direction	Calendar Name	Index	Func. Block	Use	ID
[-]	1	In	calendar			1	1030
	1.1		Holidays				1032

3. Right-click and select **Configure Pattern ...** in the context menu.
4. The **Configure Pattern** dialog appears as shown in Figure 101. Add dates to the calendar pattern by entering a Date Configuration. Then click **Add Entry**. The date appears in the **Pattern Entries** list on the right-hand side.
5. Edit an exception by selecting the pattern entry in the **Pattern Entries** list. Then modify the date configuration in the **Date Configuration** group box.

Configure Pattern

Pattern Name:

Create New Pattern Entry:
☒ Date ☐ Date Range ☐ Week and Day

Date Configuration:
Year:
Month:
Day:

Pattern Entries:

Type	Pattern Entry
Date	14th of July of every year

☒ Preview All ☐ Preview Selected

Preview:

February 2008	March 2008	April 2008	May 2008	June 2008	July 2008
S M T W T F S 27 28 29 30 31 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

August 2008 September 2008 October 2008 November 2008 December 2008 January 2009

Figure 101: Configure Calendar Pattern Dialog.

6. Click **Save Changes** when all exception days have been entered.

Tip! *If not sure, how a date configuration affects the calendar days, click on a pattern in the **Pattern Entries** list and the affected days will be highlighted in the **Preview**.*

6.11.7 Configure Embedded Exceptions

Besides exception days of the calendar, special exception days can be embedded into the scheduler. These embedded exception days are not visible or accessible in other scheduler objects.

To Configure an Embedded Exception

1. Open the **Configure Schedule** dialog to configure daily schedules as described in Section 6.11.4.
2. Click on the **Create** button below the **Weekly/Exception Schedule Configuration** list

Weekly / Exception Schedule Configuration			
Weekday / Exception	Priority	Events	Use
Mon	-	2	☒
Tue	-	0	☒
Wed	-	0	☒
Thu	-	0	☒
Fri	-	0	☒
Sat	-	0	☒
Sun	-	0	☒
Holiday	126 (lowest)	0	☒
Maintenance Days	126 (lowest)	0	☐

Create Configure Remove

3. The **Create Pattern** dialog opens. You can enter exactly one pattern entry for the embedded exception. It is recommended to choose a descriptive name for the day, e.g. '24_12'xx' for every 24th of December.
4. Click **Create Pattern**. The embedded exception is now available.

Sun	-	0	☒
24_12_xx	0 (highest)	0	☐
Holiday	126 (lowest)	0	☒
Maintenance Days	126 (lowest)	0	☐

6.11.8 Configure Control Data Points

A scheduler object can be configured to use special control data points. An *enable/disable* data point can be configured, which enables or disables the scheduler depending on its Boolean value. An *enable/disable feedback* data point is updated with the current enabled state of the scheduler. This also reflects and an enable from the network. The *Preset Name* data point can be attached to be updated with the name of the currently active preset.

To Configure Control Data Points

1. Open the **Configure Schedule** dialog to configure daily schedules as described in Section 6.11.4.
2. Go to the **Scheduled Datapoints** tab.
3. In the Control Datapoints group box, click the  button to add the desired control data point. A data point selection dialog opens.
4. Select a matching data point and click **OK**. For the preset name a string data point must be selected.
5. To remove an undesired control data point, click on the **Remove** button.

6.11.9 Using the SNVT_tod_event

The SNVT_tod_event can be used in a schedule for implementing the next-state feature. The parts of this network variable contain:

- Current state: This is the currently scheduled occupancy state.
- Next state: This is the next, future occupancy state in the schedule.
- Time to next state: This part reflects the time in minutes until the next state becomes active.

To Use a SNVT_tod_event

1. Create a SNVT_tod_event in the data point configuration.
2. Add the SNVT_tod_event to the scheduled data points of a scheduler as described in Section 6.11.4.
3. All three parts of the SNVT_tod_event are scheduled.

No.	OPC	Direction		Datapoint Name
1	☒	Out		nvoTodEvent
1.1	☒	Out		current_state
1.2	☒	Out		next_state
1.3	☒	Out		time_to_next_state

6.11.10 Using the Local Scheduler

Once the setup of the local scheduler is done, it is basically operational. It will immediately start to work based on the configuration data downloaded through the configuration software. You can verify the daily schedules and values of scheduled data points on the Web UI (see Section 4.2.13). The local schedule can be altered over the Web UI or over the network using the underlying networking protocol.

6.11.11 Limitations for Local CEA-709 Schedulers

CEA-709 schedulers and the CEA-709 calendar adhere to the LONMARK standard objects. For CEA-709, certain restrictions exist that need to be kept in mind. Attached data points can either represent an entire NV or individual elements of a structured NV. CEA-709 schedulers may have several different groups of data points attached, i.e., the value preset may consist of more than one element. For example, a CEA-709 scheduler might schedule a SNVT_temp and a SNVT_switch and have 3 elements in each value preset as depicted in Figure 102.

Datapoint	Description	Location	Group	Default	day	night
nvo_setpoint		LINX-110.CEA709 Port.Datapoints	-	0.00	21.00	16.00
nvo_switch.value		LINX-110.CEA709 Port.Datapoints	-	0.00	0.00	50.00
nvo_switch.state		LINX-110.CEA709 Port.Datapoints	-	0.00	0.00	1.00

Figure 102: Example value presets in CEA-709 schedulers.

Priorities of exception days in a CEA-709 scheduler range from 0 (the highest) to 126 (the lowest). The value 127 is reserved as a default for weekdays.

Further, the implementation as LONMARK standard objects requires the use of configuration properties. If the number of CEA-709 schedulers or their capacities for daily schedules and value presets is changed, the resource and static interface of the CEA-709 port changes. The resources reserved for LONMARK calendar and scheduler objects can be changed in the project settings (see Section 6.3.4). When downloading a project, the software verifies if sufficient resources have been configured. If it detects a problem, the user is notified to update the project settings. The Auto-Set feature automatically selects the right amount of resources.

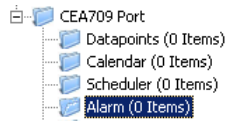
6.12 Local Alarming

6.12.1 Create an Alarm Server

To generate local alarms, an alarm server needs to be created at first. The local alarm sources will report alarms to that alarm server. The alarm server is the interface to access local alarms. This can be done over the network or the Web UI.

To Create an Alarm Server

1. Under the port folder, select the **Alarm** sub-folder to create an alarm server.



2. Right-click in the data point list view and select **New Alarm Server ...**.
3. In the **Create New Alarm Server** dialog box (as shown in Figure 103) enter **Name** and **Description** of the alarm server.

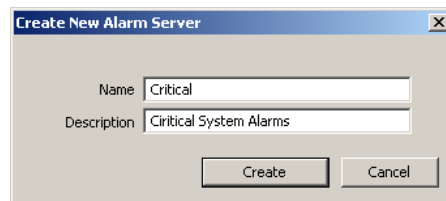


Figure 103: Create New Alarm Server dialog box.

4. Click **Create**. The alarm server appears now in the data point list view.

6.12.2 Create an Alarm Condition

To generate alarms from data points, intrinsic reporting is used. For each data point an alarm condition must be defined. This condition employs an intrinsic algorithm to generate alarms based on the data point's value. Depending on the data point type (analog, binary, multi-state), different conditions are defined. The alarm is reported to the attached alarm server.

To Create an Intrinsic Alarm Condition

1. Select a data point.
2. Right-click and select **Create Alarm Condition...** from the context menu.
3. For an analog data point, the dialog as shown in Figure 104 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select **Low Limit** and **High Limit** and put check marks, if they shall be employed. Enter a **Deadband** to account for hysteresis.

Figure 104: Alarm Condition for an Analog Data Point.

4. For enable, deadband, low limit and high limit data points can be attached by clicking the button. Those data points are used by the device to determine the actual values at run-time.
5. For a binary data point, the dialog as shown in Figure 105 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm Value** which triggers the alarm.

Figure 105: Alarm Condition for a Binary Data Point.

6. For enable, a data point can be attached by clicking the button. This data point is used by the device to determine the actual values at run-time.

- For a multi-state data point, the dialog as shown in Figure 106 appears. Select the **Alarm Server**. Optionally, enter an **Alarm Description**. If left empty, the description of the data point is used. Enter a **Time Delay**, after which the condition is evaluated. Select the **Alarm States**, which triggers the alarm, by clicking the arrow buttons.

Figure 106: Alarm Condition for a Multi-State Data Point.

- For enable, a data point can be attached by clicking the  button. This data point is used by the device to determine the actual values at run-time.
- Click on **Create**. In the alarm column, the alarm sign  will be added for those data points that have an alarm condition.

6.12.3 Deliver Alarms via E-mail

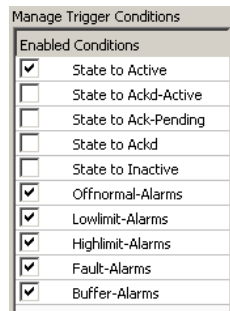
Updates in the alarm summary of an alarm object can be used as a trigger to send e-mail. For setting up e-mails, the account information has to be configured on the device, e.g., on the Web UI (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**). Then an e-mail template can be created and the alarm point attached as a trigger.

To Create an E-mail Template for Alarms

- Create or configure an e-mail template as described in Section 6.10.1.
- Change to the **Mail Triggers** tab.
- Click the **Add...** button and select an alarm data point.
- In the Mail Triggers list select the added trigger data point.

Mail Triggers		
Datapoint	Type	Condition
Critical	Alarm	-

- In the **Manage Trigger Conditions** list put a check mark on alarm conditions that shall invoke the transmission of the e-mail.



6. Change to the **Common E-Mail Properties** tab.
7. Add the alarm data point as a data source and insert the place holder into the e-mail text as described in Section 6.10.1.

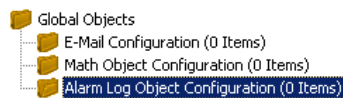
6.12.4 Create an Alarm Log

The alarm objects on the device contain an alarm summary (live list) of currently active and acknowledge-pending alarms. As soon as an alarm becomes inactive and has been acknowledged, it disappears from the alarm summary. To store a historical log of alarm transitions an *alarm log* needs to be created.

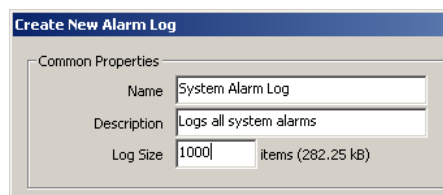
An alarm log can log transitions of one or more alarm objects. Its size is configurable. The alarm log is a ring buffer. As soon as its size limit is reached, the oldest alarm log records are overwritten by new alarm transitions.

To Create an Alarm Log

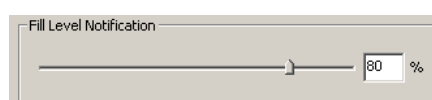
1. Under the **Global Objects** folder, select the **Alarm Log Object Configuration** sub-folder.



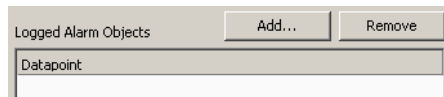
2. In the data point list right-click and select **New Alarm Log ...** from the context menu.



3. In the **Create New Alarm Log** dialog enter a **Name** for the alarm log. Optionally enter a **Description**.
4. Enter a **Log Size**, which defines how many transitions are resident in the alarm log.
5. Define a percentage for **Fill Level Notification**, which can be used to trigger the transmission of E-Mails.



- Click on the button **Add...** on top of the **Logged Alarm Objects** list.



- A data point selector dialog opens. Select one or more alarm objects that shall be logged and click **OK**. The alarm objects appear in the list.
- Click **Create** to create the alarm log object.

6.12.5 Limitations for CEA-709 Alarm Servers

Local CEA-709 alarming supports only one alarm server object. This alarm server object is represented by the device's LONMARK node object and facilitates the SNVT_alarm2 output network variable. Acknowledging alarms in the alarm server is adhering to the LONMARK specification and relies on the RQ_CLEAR_ALARM mechanism.

6.13 Local Trending

6.13.1 Create a Local Trend

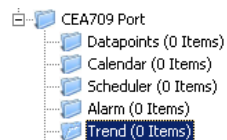
The value of a data point can be logged over time. This is referred to as trend data. To generate trend data a trend object has to be created. The trend data is stored in a data logger file. This file can be downloaded via FTP in binary or CSV format (see Section 12.1.2).

CEA-709 trend objects can generate trend logs for multiple data points and can be operated in one of three basic modes:

- Interval Mode:** In this mode a snapshot of all trended data points is logged into the data logger file.
- COV Mode:** In this mode, each of the trended data points is logged separately, if and only if its value changes. For analog data points, a specific COV increment can be configured in the data point configuration properties of the trended data point.
- Trigger Mode:** In this mode a snapshot of all trended data points is logged each time a trigger condition fires. The trigger condition is applied to a trigger data point.

To Create a Trend Object

- Under the port folder, select the **Trend** sub-folder to create a trend log object.



- Right-click and select **New Trend ...** from the context menu.
- In the **Create New Trend Object** dialog (shown in Figure 107) enter a name and optionally a description for the trend log object.

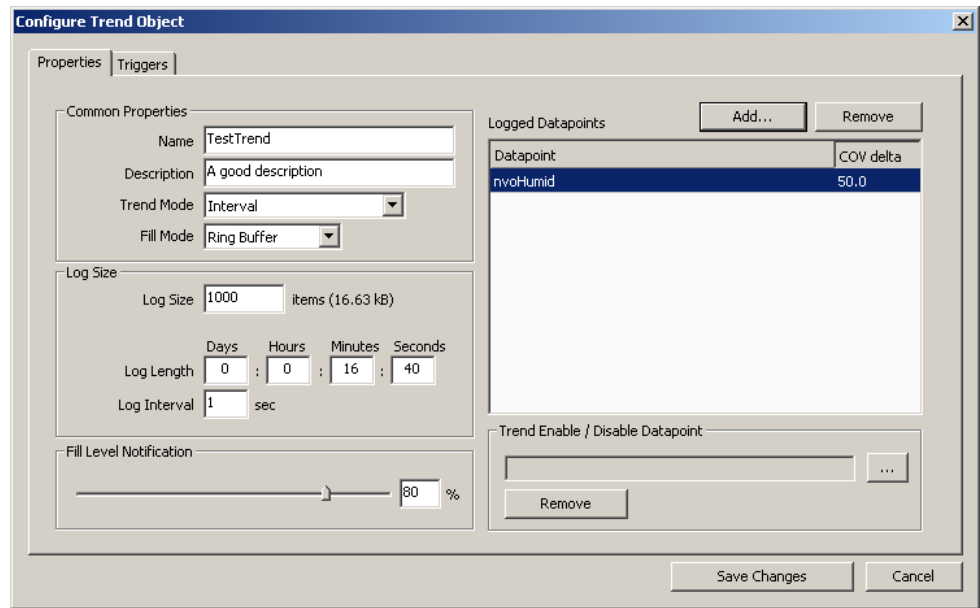


Figure 107: Basic Trend Object Configuration.

4. Select the desired **Trend Mode**.
5. Select the **Log Size**. The display in the dialog will adapt the estimations for needed data logger file size in KB and duration of the trend log. Alternatively, for interval trends, the estimated log duration and log interval can be edited.
6. Select a **Fill Level Notification** percentage. This will decide at which fill-level trigger will fire. A fill-level trigger can be used to trigger the transmission of an e-mail (see Section 6.13.5).
7. Click **Save Changes** to store the basic configuration of the trend object. The new trend log object appears in the data point list of the Trend folder.

6.13.2 Configure Trended Data Points

When a local trend object has been created, it needs to be configured, which data points it shall log. This is done by attaching data points to the trend object. Only simple data points can be attached for trending, i.e., of class analog, binary, or multi-state. For trend log objects in the CEA-709 technology, multiple data points can be attached for trending.

The trending can be enabled/disabled on behalf of an *enable* data point. This data point should be of type *binary*. If the value of that enable data point is TRUE, the trend object logs data as defined by the trend mode. If the value of the enable is FALSE, trending is disabled. If no enable data point is configured, the trend log is always enabled.

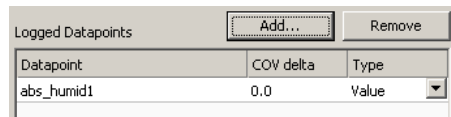
To Attach Data Points for Trending

1. Select the trend object in the Trend sub-folder.

No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

2. Right-click and select **Configure Trend** from the context menu. The same dialog which appears when a new trend object is created is shown and allows configuring the trend object. Of course, this step can also be done directly when the object is created.

3. Add data points to be trended. Click on **Add ...** which opens a data point selector window.



4. Select the data points and click **OK**. For each of the attached data points, a line appears in the list below the add button. The trended data points will also appear with the trend icon  in the data point manager.

Tip!

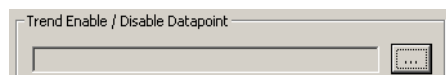
Data points can also be attached to a trend by selecting a data point in the data point manager, drag it onto a trend object and drop it on the trend object.

5. Data points can be removed from the trend by clicking **Remove**.
6. If COV mode was selected, the COV increment is displayed in the **COV delta** column. This value can be increased to produce less trend data. Note, that it cannot be lowered under the trended data point's own COV increment. Go to the data point configuration to change the COV increment in this case.
7. If the trended value of the data point shall be aggregated over the log interval, select the desired aggregation in the **Type** column. Available options are **Min**, **Max**, **Avg**.

Tip!

For creating multiple curves with min, average, and maximum values, add the same data point three times and select the different aggregation types.

8. In addition, a special **Trend Enable** data point can be selected. If configured, the trend log will only log data, if the value of this data point evaluates **true**, i.e., is not zero. Click the ... button to select a data point.



9. To remove the enable data point, click the **Remove** button.
10. When done with the data point setup, click **Save Changes** to leave the dialog.

Tip!

*A shortcut to creating a trend log object and attaching a data point is to select a data point in the data point manager, right-click on it and choose **Trend Datapoint** from the context menu. This generates a trend log and links that data point to it.*

6.13.3 Trend Triggers

Local trend objects in CEA-709 can be operated in *trigger mode*. In this mode, one or more trigger data points cause the generation of a snapshot containing the values of the trended data points at the time instant the trigger is activated. For a trend object, one or more trigger conditions can be defined. Depending on the trigger data point type, the trigger conditions can be refined.

Note, that the behavior of the trigger data point is influenced by the COV properties of the data point. If the **Only notify on COV** property is checked, the data point triggers only if its value changes to the value of the trigger condition. If that property is not checked, the data point triggers on every write with a value that matches the trigger condition.

To Configure Trigger Data Points for Trending

1. Select the trend object in the **Trend** sub-folder.

No.	Direction	Trend Name	Use	ID
1	Out	TestTrend	0	1014

- Right-click and select **Configure Trend** from the context menu.
- Change to the **Triggers** tab.

Note: Of course, you can also change directly to the **Triggers** tab when creating a trend object.

- Click the **Add...** button. A data point selection dialog opens.
- Select one or more data points and click **OK**.
- The triggers appear now in the **Trend Triggers** list.

Trend Triggers			Add...	Remove
Datapoint	Type	Condition		
state	Value Update	-		

- In the **Manage Trigger Conditions** you can refine the trigger condition depending on the trigger data point class.
- When done with the data point setup, click **Save Changes** to leave the dialog.

6.13.4 Download Trend Data in CSV Format

Trend logs can be downloaded from the device via FTP in CSV format (see Section 12.1.2). The CSV contents are generated on-the-fly from the internal binary storage when accessing the file. Each trend log point has one CSV file. The files are located in
 /data/trend/TrendLogName_UID.csv

Where *TrendLogName* is the data point name of the trend (Trend Name). The *UID* is the unique ID of the trend log object. The UID can be obtained from the ID column in the data point list of trend log data points as shown in Figure 108. This would result in the trend CSV file '/data/trend/out_temp_107C.csv'.

No.	Direction	Trend Name	Object Name	Obj Type	Instance	Alloc	Use	ID
1	Out	out_temp	out_temp	Trend Object	26	50	0	107C

Figure 108: UID of data points.

Because the contents are generated on-the-fly, the file size in the FTP client will appear as 0 Bytes. The decimal point and CSV column separator can be configured in the system configuration of the Web UI (see Section 4.2.1). Note, that for a comma “,” as the separator, the decimal point is a point. This is useful for English/U.S. applications. For countries that use the comma as the decimal point, select the semicolon as the CSV separator.

6.13.5 Deliver Trend Data via E-mail

Trend logs can be downloaded from the device via FTP. This requires an active action by the user. Alternatively, trend data can be sent as an e-mail attachment. For doing that, an e-mail template has to be setup for the trend log to be transmitted. The fill-level condition in the trend object can be used as a trigger to send an e-mail with the trend's data logger CSV file as an attachment.

For setting up e-mails, the account information has to be configured on the device, e.g., on the Web UI (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**). Then an e-mail template can be created and the trend object attached as a trigger.

To Create an E-mail Template for Trends

1. Create or configure an e-mail template as described in Section 6.10.1.
2. Change to the **Mail Triggers** tab.
3. Click the **Add...** button and select a trend object.
4. In the **Mail Triggers** list, the added trigger data point appears with the **Fill Level** condition.

E-Mail Triggers		
Datapoint	Type	Condition
TestTrend	Fill Level	

5. Change to the **Attachments** tab.
6. Select the trend log CSV file of the trend object in the **Attach File** drop-down box and click **Add**.

Note: ZIP versions of the CSV files are also available. Select those to save transmission bandwidth and mailbox space.

Attachments		Attach File	TestTrend_1014.csv	Add
Attachment	Device File Path	Add Datetime		Remove
TestTrend_1014.csv	/tmp/uid/trend/1014.csv	☒		

7. Click **OK** to complete the e-mail template configuration.

6.13.6 Limitations for Local CEA-709 Trends

Local CEA-709 trend objects support trending multiple data points in all trend modes, interval, COV, and trigger. The enable data point is also supported. All data points can be NVs, registers or of any other technology. There is no LONMARK object linked to the trend object. Consequently, trend data cannot be accessed over a LONMARK mechanism.

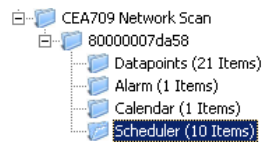
6.14 Remote AST Objects

6.14.1 Remote Scheduler and Calendar

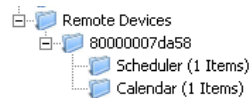
Adding remote access to the configuration of a scheduler and calendar, which is located on another device, is done by creating remote scheduler and calendar objects. These objects can be created from data obtained by a network scan or LNS scan.

To Create a Remote Scheduler

1. Execute a network scan, as described earlier in this document. The scan folder is filled with available schedulers.



- From the data points in the import folder, select the scheduler objects you are interested in and click the  **Use on Device** speed button. This creates suitable remote schedulers and the corresponding calendar objects in the **Remote Devices** folder.



- Adjust the basic settings for the newly created objects, such as the object name and description. The object name will be used as the name for the scheduler, as seen on the Web UI.
- A static NV is created to receive information from the remote device about changes to the scheduler configuration, so that the local device does not need to poll the remote device. Set a name for this NV (default is `nviSchedLink<number>`) and assign it to a suitable function block.

Note:

Due to the static input NV, which is required for a remote CEA-709 scheduler object, adding remote scheduler points will change the static interface of the device.

The new static input NV representing the remote calendar on the local device (this NV is normally called `nviCalLink`) needs to be bound to the output NV called `nvoCalLink` located in the Calendar functional block of the remote device and the new static `nviSchedLink` NVs which were created for each remote scheduler point need to be bound to the respective `nvoSchedLink` variable located in the Scheduler functional block of the remote device. The binding between the `nvoSchedLink` variable on the remote device to the `nviSchedLink` variable on the local device defines which of the scheduler data points on the local device connect to which scheduler unit on the remote device. All required information is transmitted over the link NVs, so it is possible to later change the binding to any other remote scheduler without rescanning the network.

Note:

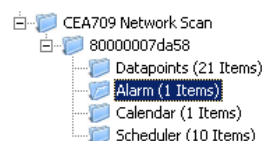
If connected via LNS, the bindings to the `nvoCalLink` and `nvoSchedLink` NVs are made automatically by the configuration software in the download process.

6.14.2 Alarm Clients

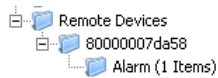
Accessing alarm server objects on remote devices is done by creating remote alarm data points. These points may be created from data obtained by a network scan. The local device is configured as an alarm client and subscribes to alarm updates from the remote alarm server. The alarm client can also be used to acknowledge alarms on the remote alarm server. Any updates are synchronized back to the alarm client.

To Create an Alarm Client

- Execute a network scan, as described earlier in this document. The scan folder is filled with available remote alarm servers.



- From the points in the import folder, select the alarm server points you are interested in and click the  **Use on Device** speed button. This creates the corresponding alarm client points in your project.



- Select the new alarm client point and adjust the name of the local NV (default name is `nviAlarm_2`). This NV is located in the *Clients* functional block.

Note: Due to the static input NV which is required for a CEA-709 alarm client point, adding alarm clients will change the static interface of the device.

The new static input NVs representing the alarm clients on the local device need to be bound to the alarm outputs of the remote device. A CEA-709 device normally delivers alarms through an output NV of type `SNVT_alarm_2` located in the node object of the device, therefore the new input NV on the local device must be bound to the alarm output NV of the remote devices node object. All required information is transmitted over the alarm input NV, so it is possible to later bind the alarm client to any other alarm server without rescanning the network.

Note: If connected via LNS, the binding to the `nvoAlarm2` NV is made automatically by the configuration software in the download process.

6.15 Math Objects

6.15.1 Create a Math Object

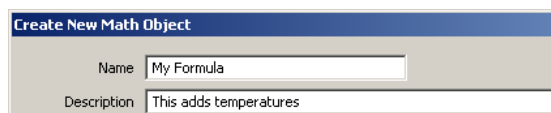
Math objects are advanced application objects that can execute mathematical operations on data points. A math object takes a number of input data points (variables $v_1, v_2, \dots, v_n$) and calculates a result value according to a specified formula. When configuring a math object, the input data points, output data points and the formula must be configured by the user. Input data points can be configured with a change-of-value condition, to trigger the math calculation only if the value changes more than a certain delta.

To Create a Math Object

- Under the **Global Objects** folder, select the **Math Object** sub-folder.



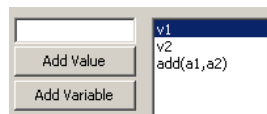
- Right-click and select **New Math Object ...** from the context menu.
- In the **Create New Math Object** dialog, enter a name and optionally a description for the math object.



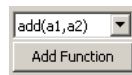
- Attach input data points by clicking the **Add Input DP** button.

Add Input DP... Remove Input DP Replace Input DP... Detach Input DP			
Var.	Input Datapoint	Datapoint Path	COV delta
v1	nviTemp1	LINX-100.CEA709 Port.Datapoints	0.0
v2	nviTemp2	LINX-100.CEA709 Port.Datapoints	0.0

- In the data point selector dialog, select the input data points and click **OK**. The data points appear as v1, v2, etc.
- If the data point shall trigger the math calculation only after a certain change-of-value, enter a value into the **COV delta** column.
- Select the input data point and click **Add Variable** to push the variable on the evaluation stack.



- Select a function to be applied on the variables and click the **Add Function** button.



- The resulting formula is displayed at the bottom of the dialog. Alternatively, the formula can be entered there.



- Add output data points by clicking the **Add Output DP** button.

Add Output DP Remove Output DP	
Output Datapoint	Datapoint Path
my_register_Write	LINX-100.User Registers

- In the data point selector dialog select the output data points and click **OK**.
- To create the math object click **Create**.

6.15.2 Editing a Math Object

Math objects can be edited once created. The formula can be changed, new variables added, or additional output data points added.

To Edit a Math Object

- Under the **Global Objects** folder, select the **Math Object** sub-folder.



2. Select the math object in the data point list.

Math Objects			Datapoint Name Filter:		
No.	Direction	Name	Description	ID	
1		My Formula	This adds temperatures	1000	

3. Right-click and select **Configure Math Object ...** from the context menu.
4. Edit the math object as described in Section 6.15.1.
5. To replace an input data point by another input data point without re-writing the entire formula, click the **Replace Input DP ...** button. This opens a data point selector dialog. Select the replacement data point there.
6. To detach an input data point click the **Detach Input DP** button. This leaves the respective variable slot empty.
7. To finalize the edit click on **Save Changes**.

7 The LINX-101 Router

The LINX-101 is equipped with a standard CEA-709 router (i.e., an embedded L-IP), which connects the FT port and the CEA-852 port. Depending on the use case, the LINX-101's router supports different operating modes how packets are routed between the CEA-709 side and the IP-852 side. The LINX-101 also contains a configuration server (CS) to manage members on an IP-852 channel.

7.1 CEA-709 Router

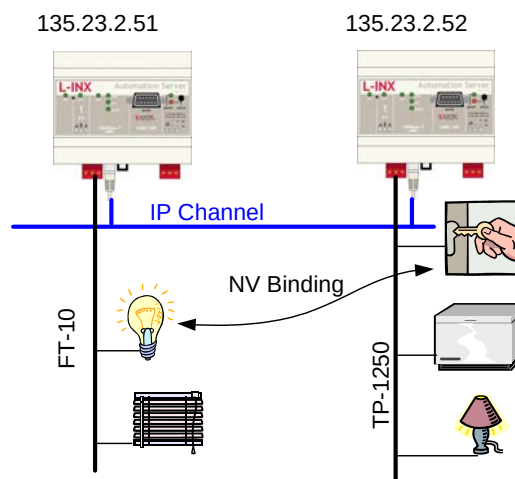


Figure 109: The LINX-101 supports different methods to route packets between the CEA-709 and IP-852 channel.

Depending on the CEA-709 router configuration (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**) the LINX-101 supports 4 different methods to route packets between the CEA-709 and the IP-852 channel. The 4 operating modes are listed below and described in more detail in the subsequent sections.

- Configured Router: The LINX-101 acts like a standard CEA-709 configured router (i.LON 1000/600 alike)
- Smart Switch: The LINX-101 acts as a self-learning plug&play router (“smart switch mode”)
- Store-and-Forward Repeater: To freeze a learned configuration and operate the switch based on the existing forwarding tables, disable group learning and Subnet/Node learning.

- Smart switch with no broadcast flooding: Set Subnet/Node Learning to “subnet”. In this mode the LINX-101 learns the network topology but doesn’t flood subnet broadcasts.

7.1.1 Configured Router Mode

In this operating mode, the LINX-101 acts like a standard configured router, which can be configured with standard network management tools like LonMaker or NL-220. This operating mode is compatible with the *i.LON* 1000 and the *i.LON* 600.

This operating mode uses the “channel routing” routing strategy on the IP channel. In this mode the LINX-101 is fully compatible with *i.LON* 1000/600 devices. This operating mode should also be used in networks with more than 10 IP devices on one IP channel and heavy network traffic on the IP channel (more than 500 packets/s) since channel routing sends the IP packet only to the LINX-101 device(s) that connect to the CEA-709 node(s) addressed in this IP packet and not to all LINX-101 devices on the IP channel. This is the standard operating mode.

7.1.2 Smart Switch Mode

The LINX-101 can be configured to act as a learning switch in a CEA-709 network. This operating mode is called smart switch mode. In this operating mode, the LINX-101 decides if the message has to be forwarded or not, based on the destination address of a message. Thus, it isolates local network traffic (e.g., in case of heavily loaded networks).

Important: ***This operating mode doesn’t support network loops!***

Important: ***Whenever a network is reconfigured, it is recommended to clear the forwarding tables in the LINX-101 by pressing the status button for at least 20 seconds (see Section 3.5.1).***

The router supports learning of up to 4 Domains.

Note: *All messages, which are received on an unknown domain, are forwarded to all ports!*

The subnet/node learning algorithm supports segmentation of the network traffic on a subnet/node basis. Thus, the user does NOT need to take care of any subnets spanning multiple physical channels. Even when a node is moved from one channel to another, the LINX-101 keeps track and modifies its forwarding tables accordingly.

Note: *All messages with a destination subnet/node address not yet learned are forwarded!*

The router supports group learning. Groups can span multiple router ports.

Note: *Group learning only works for messages using acknowledged or request/response service.*

Note: *All messages with a destination group address not yet learned are forwarded!*

The router has no learning strategy for broadcast addresses. As a result, all subnet or domain wide broadcasts are always forwarded. If subnet wide broadcasts shall not be forwarded, please use the smart switch operating mode without subnet broadcast forwarding (see Section 7.1.4).

The router has no learning strategy for unique node ID addresses. Node ID addressed messages are always forwarded.

This operating mode uses the “channel routing” strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn’t scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 IP-852 devices and packet rates of more than 500 packets/s. Please use the configured router mode from Section 7.1.1 for larger IP channel configurations.

Further, it is recommended to configure a multi-cast group for routers in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 7.5 on how to configure the LINX-101 to use multi-cast.

7.1.3 Store-and-Forward Repeater

The router can be configured to operate in a repeater mode, where all messages are forwarded regardless of the address format.

This operating mode uses the “channel routing” strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn’t scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 router devices and packet rates of more than 500 packets/s.

Further, it is recommended to configure a multi-cast group for routers in repeater mode to reduce the traffic burden and improve scalability. Refer to Section 7.5 on how to configure the LINX-101 to use multi-cast.

7.1.4 Smart Switch Mode with No Subnet Broadcast Flooding

This operating mode is the same as the smart switch mode from Section 7.1.2 with the only difference that subnet wide broadcasts are not flooded in this mode. This operating mode can be used in large network installations where the network management tool uses group overloading to replace group addresses with subnet wide broadcasts. In this operating mode, the network installer must ensure that one subnet address may only exist behind one and no more than one network port. This condition is met if nodes are installed using an LNS based tool, on different channels that are separated with a router shape.

This operating mode uses the “channel routing” strategy on the IP channel to distribute IP packets. It uses flooding to send all packets on the IP channel to all IP devices on this IP channel. The advantage of this operating mode is that it is fully plug&play and no router configuration is required. The disadvantage is that this operating mode doesn’t scale very well with larger networks. We do not recommend this operating mode for IP channels with more than 10 devices and packet rates of more than 500 packets/s.

Further, it is recommended to configure a multi-cast group for the router in the smart switch mode to reduce the traffic burden and improve scalability. Refer to Section 7.5 on how to configure the LINX-101 to use multi-cast.

7.2 CEA-852 Device of the Router

Every LINX-101 acts as a device on the IP channel. It either needs to contact a configuration server or a configuration server needs to contact the device in order to set up the proper routing tables. Before a device can become a member of the IP-852 channel it needs to have proper IP settings (see Section 4.2.4):

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.2.4

- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.2.6
- MD5 secret if authentication is required, see Section 4.2.6

Please consult Sections 4.2.4 and 4.2.6 on how to setup a CEA-852 device.

The LINX-101 can be used together with the PC-based *i.LON* Configuration Server utility or with any LOYTEC configuration server. If multiple CEA-852 devices behind one NAT router are added, the Auto-NAT setting in the CEA-852 devices is recommended to be used with the LINX-101 configuration server or an L-IP configuration server. Please refer to the following sections on how to setup the device and the configuration server.

If the “Auto member” feature is enabled in the configuration server, the CEA-852 device can add itself to the IP-852 channel without explicitly adding the device at the configuration server. Note, that enabling auto member is a potential security hole since any device can add itself to the IP-852 channel.

7.3 Configuration Server for Managing the IP-852 Channel

7.3.1 Overview

Every logical IP-852 channel requires one configuration server that manages all CEA-852 devices (LINX-101, L-IP, LOYTEC NIC852, *i.LON* 1000, *i.LON* 600, LonMaker, etc.) on this channel. A simple example is shown in Figure 110. A configuration server keeps a list of all devices on a logical IP-852 channel and distributes the routing information between those devices. If a device wants to join an IP-852 channel, it needs to register itself at the configuration server. Traditionally, a dedicated Windows PC is used to act as the configuration server. The LINX-101 contains an embedded configuration server and can therefore replace the PC.

The configuration server can be enabled in the LINX-101 in the CEA-852 server configuration menu in Section 4.2.8. This configuration server can manage one IP-852 channel and up to 256 devices on this IP-852 channel. In order to setup the configuration server, one must specify the following parameters:

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.2.4
- NAT address if used behind a firewall/NAT router, see Section 4.2.6
- MD5 secret if authentication is required, see Section 4.2.6
- Enable the configuration server, see Section 4.2.8 (server LED lights up green)
- A list of IP-852 channel members, see Section 4.2.9.

Note: If the LINX-101 is used as a configuration server it needs a fixed IP address.

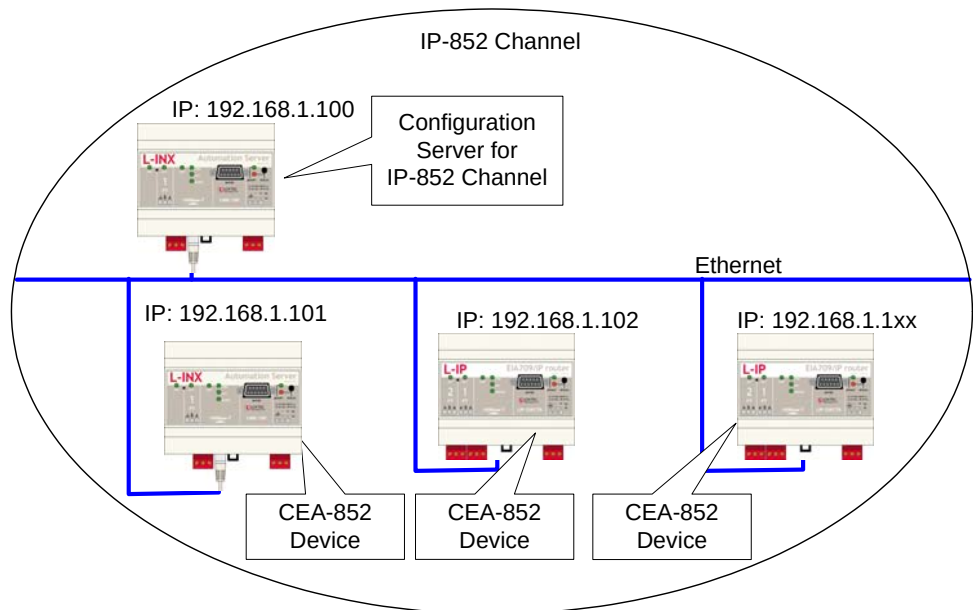


Figure 110: The configuration server manages the devices on an IP-852 channel.

7.3.2 Configuration Server Contacts IP-852 Device

In this scenario, the IP-852 device needs the following parameters set in order for the configuration server to contact the device. The remaining parameters are retrieved from the configuration server.

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.2.4
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.2.6
- MD5 secret if authentication is required, see Section 4.2.6

If multiple IP-852 devices behind one NAT router are added, the Auto-NAT setting in the LINX-101 is recommended to be used with the LINX-101 configuration server.

7.3.3 IP-852 Device Contacts Configuration Server

In this scenario, the IP-852 device needs the following parameters set in order to contact the configuration server. The remaining parameters are retrieved from the configuration server.

- IP address/netmask/gateway (either via DHCP or manual entry), see Section 4.2.4
- Auto-NAT or manual NAT address if used behind a firewall/NAT router, see Section 4.2.6
- MD5 secret if authentication is required, see Section 4.2.6
- Configuration server IP address and port number, see Section 4.2.6

If the “Auto member” feature is enabled in the configuration server, the IP-852 device can add itself to the IP-852 channel without explicitly adding the device at the configuration server. Note, that enabling auto member is a potential security hole since any device can add itself to the IP-852 channel.

7.3.4 Using the Built-In Configuration Server

For security purposes, the configuration server contacts each IP-852 device on the IP-852 channel. Therefore, one must enter a list of all channel members in the CEA-852 Configuration Server menu (see Section 4.2.9). This ensures that no unwanted device can join the IP-852 channel. A properly configured IP-852 channel list can look like Figure 111.

```
List of channel members
=====
```

No	Name	IP Address	Status	Flags
000	local	128.168.1.253:1628	registered	

NAT Router		128.168.1.250		
+ 001	lip-n1	10.0.2.2:1628	registered	
+ 002	lip-n2	10.0.2.3:1631	registered	

003	pc37	128.168.1.37:1628	not responding	

Press <RETURN> to continue

Figure 111: Properly configured IP-852 channel with 4 channel members.

Note that also *i.LON* 1000/600, VNI and LOYTEC NIC852 based network nodes (e.g., LonMaker or NL-220 applications) can join the IP-852 channel managed by the configuration server.

Note that the built-in configuration server should be used if LINX-101 or L-IP devices are communicating across firewalls/NAT routers.

For adding multiple devices behind a NAT router, the configuration server supports the extended NAT mode (see Section 7.4.2). The configuration server automatically switches the channel mode to extended NAT if needed. Note that the *i.LON* 600 must be configured with the *i.LON* CS to extended NAT mode before adding the *i.LON* 600 to the configuration server, because the *i.LON* 600 does not switch to that mode automatically.

7.4 Firewall and NAT Router Configuration

The LINX-101's router can be used behind a firewall and/or NAT (Network Address Translation) router as shown in Figure 112. Note, that in general, only one CEA-852 device can be used behind the NAT router. This mode of operation is referred to as "Standard" channel mode. It is fully compliant with CEA-852.

LOYTEC's newer devices such as the L-IP and the LINX-101 support more than one CEA-852 channel member behind a NAT router. This mode of operation is referred to as "Extended NAT" channel mode. This mode introduces extensions to the standard mode which need to be supported by all members. Other devices supporting the extended NAT mode are the *i.LON* 600. See Section 7.3.4 on compatibility with the *i.LON* 600.

7.4.1 Automatic NAT Configuration

In order to use the LINX-101 behind a firewall, the public NAT address and the local IP address must be set in the IP configuration menu (see Section 4.2.4). By default, the NAT address is determined automatically when adding the LINX-101 to the channel in the configuration server. Alternatively, the NAT address can be configured manually. Furthermore, the NAT router must be configured to forward ports 1628 and 1629 for UDP and TCP packets to the private IP address of the LINX-101 (192.168.1.100 in Figure 112). In summary we can say, the following parameters must be set in order to operate a LINX-101 behind a NAT router.

- Specify the IP address (private IP address: 192.168.1.100),

- Specify the gateway address (e.g., 192.168.1.1),
- Specify the NAT address (public IP address: 135.23.2.1) or use automatic NAT router discovery,
- Enable port forwarding for ports 1628 and 1629 in the NAT router for TCP and UDP,
- Enable the SNTP port 123 in the firewall if SNTP is used.

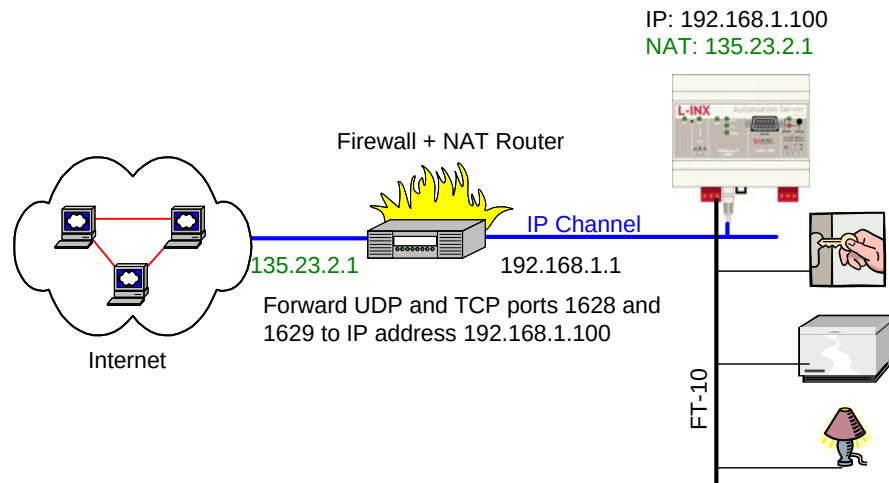


Figure 112: Operating a LINX-101 behind a NAT router and firewall.

Note that a LINX-101 must be used as configuration server when the device is installed behind a firewall or NAT router. The LINX-101 with the configuration server can also be located behind a firewall.

7.4.2 Multiple IP-852 Devices behind a NAT: Extended NAT Mode

When using more than one IP-852 device behind a single NAT router, the recommended method in the LINX-101 configuration server is to use the extended NAT mode. This mode requires that all devices support this feature. Currently these are LINX-101, L-IP 3.0, i.LON 600, the NIC852 PC software and other CEA-852 capable devices from LOYTEC. If there are other devices in the channel, this method does not work. Incompatible devices are disabled from the channel in this case. Please refer to the classic method in Section 7.4.3 to setup this network.

When using multiple devices behind a NAT router, each device needs a separate port-forwarding rule in the NAT router. This implies that each device must use a unique client port (e.g., 1628, 1630, 1631, etc). The port-forwarding rules must be setup so that each port points to one of the IP-852 devices. In the LINX-101, change the client port in the CEA-852 device configuration menu. Figure 113 shows an example configuration for three LINX-101s behind the NAT router 135.23.2.1.

It is recommended that both ports 1628 and 1629 are forwarded to the same private address. It is then also possible to turn on the configuration server behind a NAT router. In this case, activate the CS on the LINX-101 which has port-forwarding to 1628 and 1629. In the example in Figure 113, the LINX-101 with private address 192.168.1.100 also acts as a configuration server.

If the CS is activated on a LINX-101 behind a NAT router, the NAT router must have a fixed public IP address. The LINX-101 with the CS also cannot use automatic NAT discovery. In this case, enter the NAT address of the NAT router manually in the IP configuration menu (Auto-NAT can no longer be enabled on a LINX-101 with a CS). To

diagnose possible problems in the NAT configuration with port forwarding, use the enhanced communications test (see Section 4.3.3).

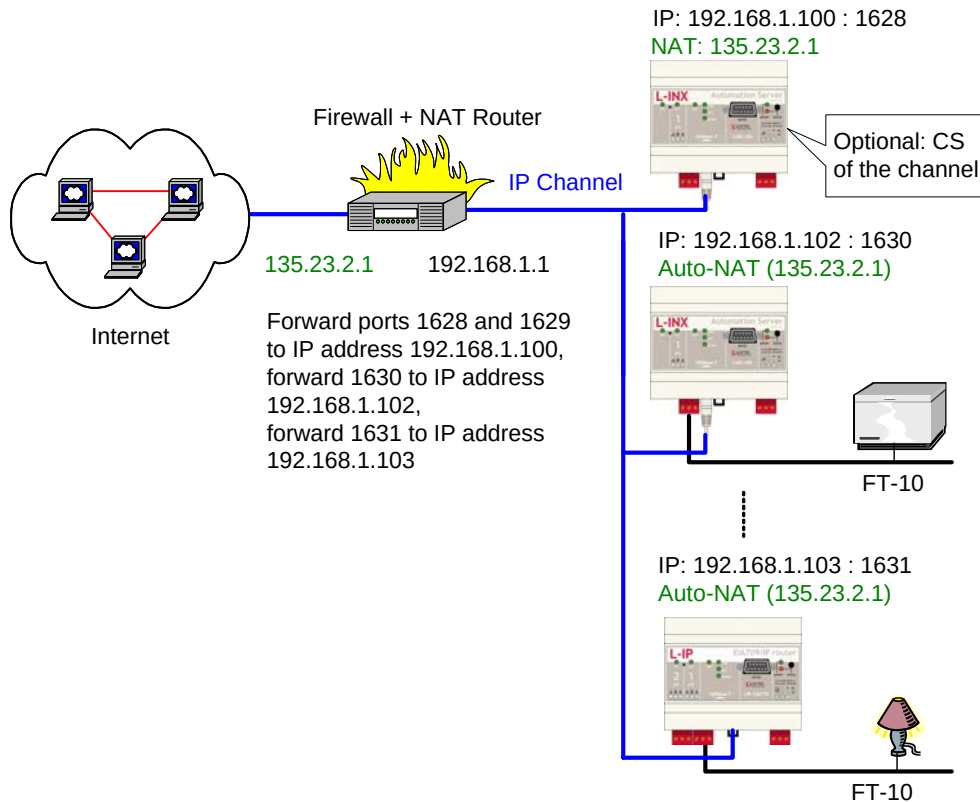


Figure 113: Multiple LINX-101 devices behind a NAT: Extended NAT Mode.

After the NAT router has been configured with the port-forwarding settings and the CS has been turned on, the channel members can be added. This can be done either on the console UI or through the Web interface of the CS.

On the console UI, add the devices to the channel in the configuration server menu 7. Choose 'a' to add a device. Enter the private address of the device in the **IP address** field. Enter the public address of the NAT router in the **NAT address** field. Modify the port as needed. For example, to add the LINX-101 with port 1631 in Figure 113, enter the values as shown in Figure 114.

CEA-852 Member Menu
=====

```
[1] IP Address      : 192.168.1.103
[2] Port           : 1631
[3] NAT Address    : 135.23.2.1
[4] Device name    : lip-103
```

```
[q] Quit without saving
[x] Exit and save
```

Figure 114: Adding a member with extended NAT Mode on the console UI.

In the Web UI, add the members with their private IP addresses and the client ports as defined by the port-forwarding. Then select the added member by checking the check box and select the action **Assign to NAT**. Enter the public NAT address of the NAT router. An example to add the two IP-852 devices in Figure 113 through the Web UI is depicted in Figure 115. To remove a device from a NAT router but not delete it, select it and choose **Remove from NAT** as the action.

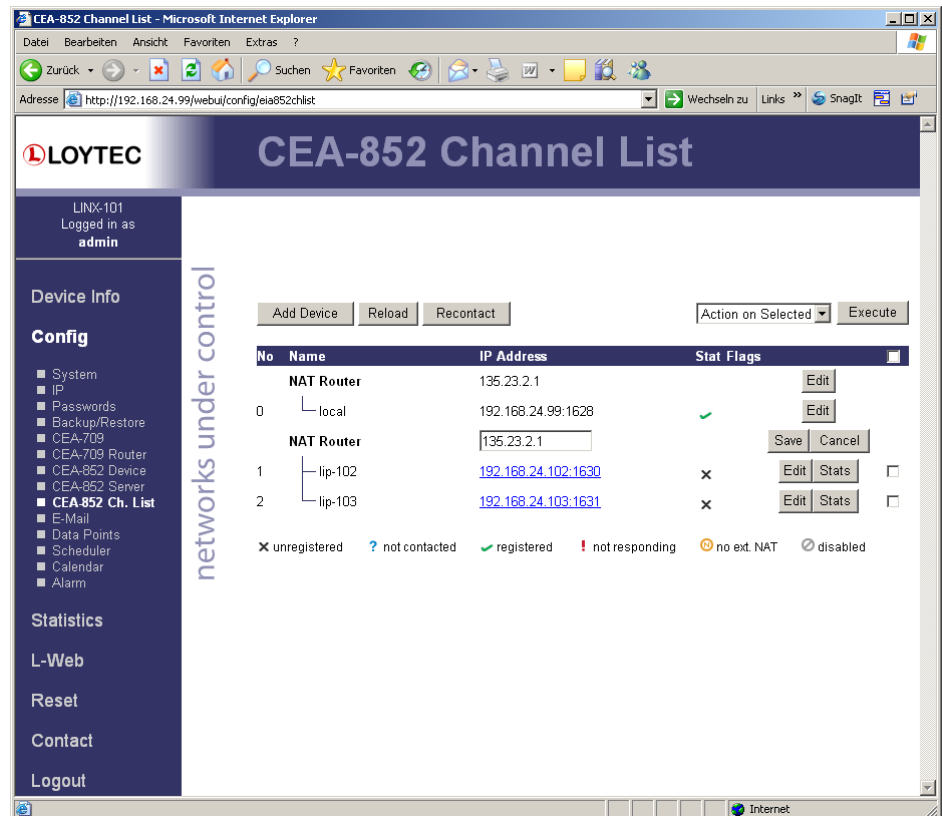


Figure 115: Adding a member with extended NAT Mode on the Web UI.

7.4.3 Multiple IP-852 devices behind a NAT: Classic Method

If more than one LINX-101 must be used behind the NAT router and there are devices which do not support the extended NAT mode, we propose the setup from Figure 116.

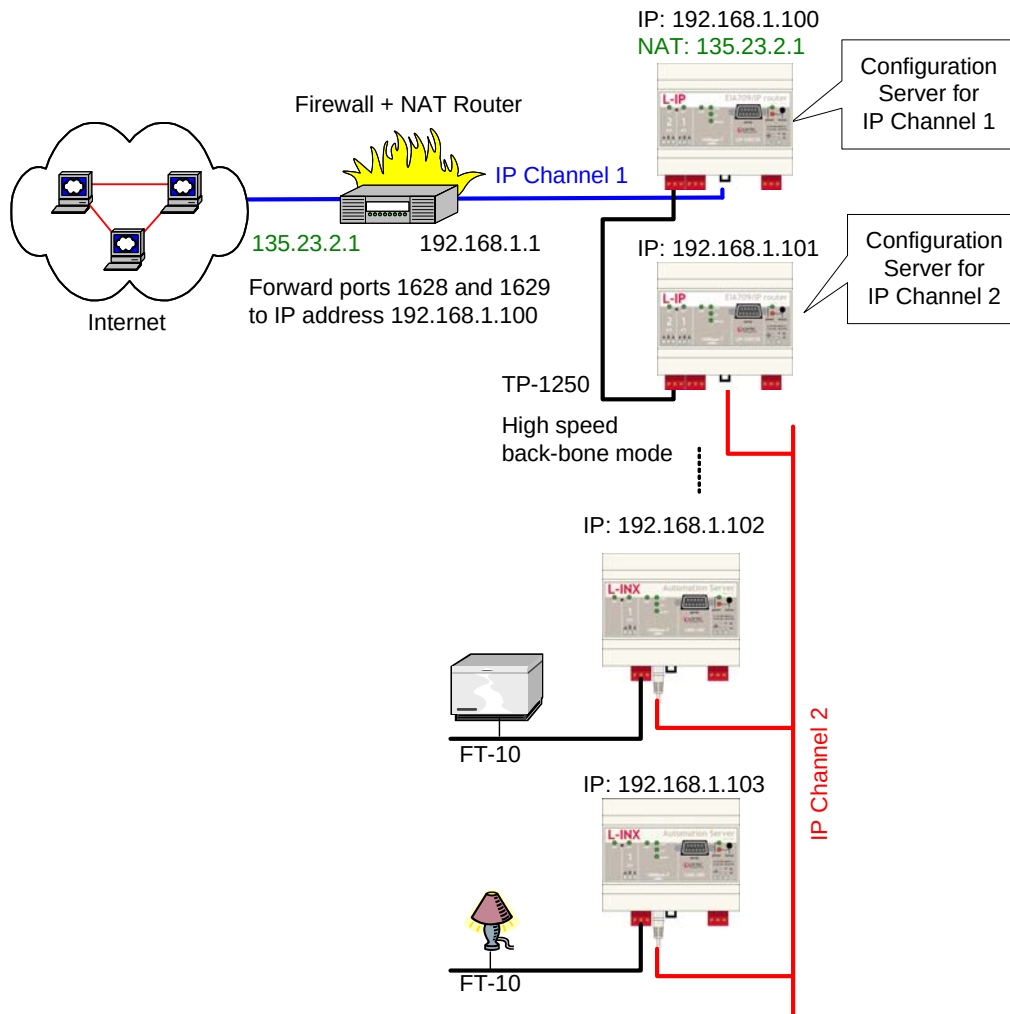


Figure 116: Application that uses multiple LINX-101 devices behind a NAT router firewall.

The LINX-101 with IP address 192.168.1.100 is member of IP Channel 1 and can be accessed through the Internet. The LINX-101 devices with IP addresses 192.168.1.101 to 192.168.1.110 form another logical IP Channel 2 that communicates with the devices on the IP Channel 1 over the TP-1250 channel, which is used in high-speed backbone mode for optimum networking performance. Note that devices on both IP Channels 1 and 2 can of course connect to the same physical network wiring. Furthermore, both IP Channels 1 and 2 must have a separate configuration server that manages the LINX-101 devices on the different channels. In the example in Figure 116, the LINX-101 with address 192.168.1.100 acts as the configuration server for IP Channel 1 and the LINX-101 with IP address 192.168.1.101 acts as the configuration server for IP Channel 2.

7.5 Multi-Cast Configuration

IP multi-casting is a feature of the IP protocol that allows one packet to be delivered to a group of IP hosts. To receive such multi-cast packets, each IP host must be member of a multi-cast group. This group is identified by a multi-cast address (e.g., 225.0.0.37) and a UDP port number.

The LINX-101 supports both unicast and multi-cast delivery of CNIP data packets. Using multi-cast is recommended when using the LINX-101's router in the Smart Switch Mode. For those LINX-101s, configure a multi-cast address in the IP configuration menu. Please contact your system administrator to obtain a valid multi-cast address for your network.

Note, that all channel members must be configured with the same multi-cast address and use the same client port (1628 is recommended). Also note, that multi-cast addresses cannot be routed on the Internet. They can only be used in a LAN or VPN environment.

If you configure multi-cast, there may be some devices, which do not support this feature. In this case, the LINX-101 uses a hybrid scheme and sends unicast to those devices, which are not configured for multi-cast. Note, that the LINX-101 determines automatically, when to switch to the multi-cast mode depending on what types of devices are in the channel and on the traffic burden for those devices. As a rule of thumb, multi-cast is used when there are only switches/repeaters in the channel and it is not used when there are only configured routers.

To detect if the LINX-101's router utilizes the multi-cast feature, contact the Extended CEA-852 device statistics in the statistics menu (Section 4.2.6). The entry "Channel Routing Mode" reads SL (send list) if packets are routed to the multi-cast group. It reads CR (channel routing) if the normal unicast method is employed. Also the entry "Multi-cast packets sent" in the CEA-852 device statistics menu (Section 4.2.6) counts the number of multicast packets transmitted to the group. If this item remains zero, no multi-cast is used by the LINX-101.

7.6 Remote LPA Operation

The LINX-101 supports remote LPA access. This means that a CEA-709 protocol analyzer connected to the Ethernet network can connect to the LINX-101 and record all packets on the CEA-709 channel (FT-10). Our LPA-IP supports this sophisticated feature. The functionality is shown in Figure 117.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In a LINX-101 device selection window, one can e.g. select the LINX-101 with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the LINX-101 with IP address 192.168.1.210. For this operation, the LPA-IP does not need to be a member of the IP-852 channel. Note that this functionality is only available with LINX-101 Internet routers.

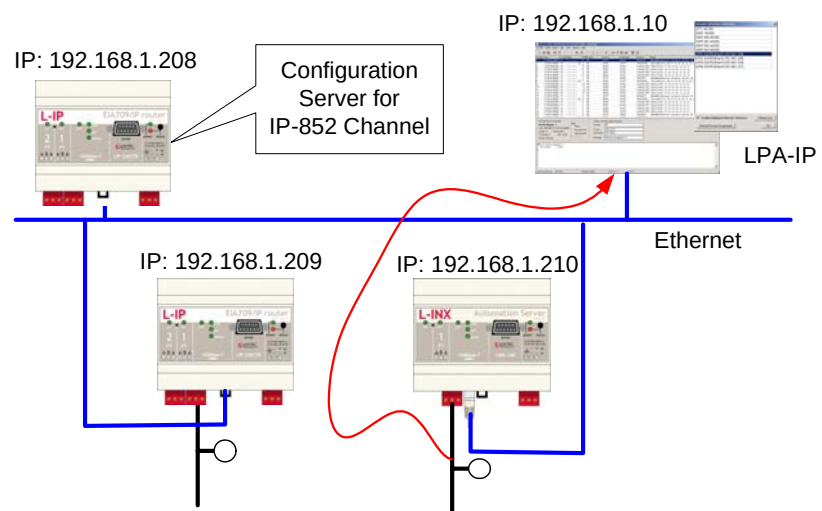


Figure 117: Remote LPA principle.

7.7 Internet Timing Aspects

If the LINX-101's router is used over the Internet or in a large Intranet with unpredictable network delays, the user should become familiar with the following advanced timing aspects. Channel Timeout is set in the configuration server whereas escrowing and aggregation are set in the CEA-852 client device. The Channel Delay is a channel property of LNS and can be set in NL-220, LonMaker or other network management tools.

Table 8 summarizes the timing values that must be set when operating the LINX-101 under WAN conditions.

Timing Parameter	Value
Channel Timeout	Average ping delay + Aggregation Timeout
Escrowing (Packet Reorder Timer)	The smaller value of: $0.25 \times \text{Channel Timeout}$ or 64ms
Aggregation Timeout (Packet Bunching)	Typically 16 ms
Channel Delay in LonMaker	Average ping delay +10% + $2 \times \text{Aggregation Timeout}$

Table 8: Advanced IP-852 timing parameters.

Please use a PC to determine the average ping delay between the different LINX-101s in the network. If multiple LINX-101s are communicating with each other always use the largest measured average ping delay for the input value for the calculations in Table 8.

Escrowing should be disabled in a LAN (0 ms). The Channel Delay in LonMaker should be set to $2 \times \text{Aggregation Timeout}$ in a LAN if MD5 is disabled.

In LANs, Channel Timeout is only required if MD5 authentication is enabled. Set Channel Timeout to 200 ms and Channel Delay to 20 ms.

7.7.1 Channel Timeout

The Channel Timeout is a property of the IP-852 channel. If a packet travels across this IP-852 channel for longer than what is specified in Channel Timeout in ms, the packet is discarded. The LINX-101 always needs to synchronize with an SNTP timeserver when a Channel Timeout is set other than 0 ms.

Channel Timeout is highly recommended if MD5 authentication is enabled in order to prevent replay attacks. Set Channel Timeout to 200 ms and Channel Delay to 20 ms in a LAN environment. Please refer to Section 4.2.8 on how to enable or disable the Channel Timeout.

If an LNS based network management tool like LonMaker or NL220 is used on a network that has channel timeout enabled, please install an NTP client program (e.g., achron4.exe) on this PC that synchronizes the PC clock to the NTP time. Otherwise the PC clock and the clock inside the LINX-101 will drift apart and communication between the PC and the LINX-101 will terminate.

7.7.2 Channel Delay

Channel Delay is an LNS channel property that specifies the expected round-trip time of a message and its response. This value is used by LNS to adjust the protocol timers in the CEA-709 nodes. Please consult the documentation for your network management tool about the Channel Delay details.

7.7.3 Escrowing Timer (Packet Reorder Timer)

The Escrowing Timer or Packet Reorder Timer is a IP-852 channel property that specifies the amount of time the device will wait for an out-of-sequence IP packet to arrive. This parameter is important in WANs like the Internet, where packets pass many routers that can change the order in which packets arrive at the destination node. The default value is 64 ms.

Do not use the Escrowing Timer in LANs since the packet order is always guaranteed in a LAN. This will add unnecessary delays, which negatively impacts the performance of your CEA-852 devices if a packet is lost or destroyed.

Whether enabled or disabled, out-of-sequence packets are never sent to the CEA-709 channel. Please refer to Section 4.2.6 on how to enable or disable escrowing.

7.7.4 SNTP Time Server

Small IP networks like LANs have a small propagation delay for packets traveling in these networks. In this case it is not necessary to specify an SNTP server.

In larger IP-852 networks like the Internet with possibly long packet delays, one must specify an SNTP server to synchronize the local clocks of the LINX-101 devices. The local clocks must be synchronized to a common notion of time in order to make CEA-852 protocol features like Escrowing (Channel Timeout) work properly.

The SNTP timeserver can be specified on the IP-852 channel level in the configuration server, which distributes the timeserver address to all CEA-852 devices on the IP-852 channel.

A primary and a secondary SNTP server can be defined please refer to Section 4.2.6 and Section 4.2.8 on how to enable the SNTP server.

7.8 Advanced Topics

7.8.1 Aggregation

Aggregation (or packet bunching) is a technique that collects multiple CEA-709 packets into a single larger IP packet. Aggregation improves overall system performance since one IP-852 packets, now carries multiple CEA-709 packets und with the same number of IP-852 transactions, more CEA-709 packets can be exchanged between LINX-101 devices thus reducing protocol overhead. The Aggregation Timeout defines the time period in ms in which the transmitting device collects the CEA-709 packets before it transmits the IP-852 packet over the IP-852 channel. Please refer to Section 4.2.6 on how to enable aggregation. Note, that aggregation adds a delay to the transactions but dramatically improves the throughput of your IP-852 channel. Use aggregation if you have a high channel load but can tolerate some additional propagation delay given by the aggregation time value.

7.8.2 MD5 Authentication

MD5 authentication is a method of verifying the authenticity of the sending device. Only devices that have MD5 enabled and use the same MD5 secret can share information with each other. If the configuration server has MD5 enabled, only devices that have MD5 enabled and use the same MD5 secret as the configuration server can join the logical IP-852 channel. Please refer to Section 4.2.6 and 4.2.8 for details.

7.8.3 Dynamic NAT Addresses

A common practice for Internet providers is to assign addresses on a per-session basis to a client. Each time a connection is established (e.g., an ADSL link is set up), the Internet provider may choose an IP address from a pool. Since this address will be the public address of a NAT router, the NAT address configured in the LINX-101 would need to be updated. The Auto-NAT feature in the LINX-101 permanently monitors the current NAT address. When the LINX-101 detects a change in the NAT address it re-registers with the configuration server using this new address. This feature requires a LOYTEC configuration server (e.g., LINX-101, L-IP) and “Roaming Members” enabled on that CS.

A consequence of this monitoring process is that the LINX-101 contacts the CS every 45 seconds to probe for the NAT address. This causes a small amount of additional traffic on the Internet link. The Auto-NAT feature also causes any shut-down connection to be re-established. The NAT monitoring functions as a keep-alive for the connection. If neither the additional traffic nor the automatic initiation of a new connection is tolerable, the Auto-NAT feature must be disabled and the NAT address configured manually. In this case, the Internet service provider needs to assign a fixed public IP address to the NAT router.

8 The LINX-100 RNI

8.1 RNI Function

The LINX-100 provides a remote network interface (RNI) function, if the LINX-100 is configured to use the FT interface (FT mode). In this mode the device provides a remote network interface, which appears like a LOYTEC NIC-IP it is intended to be used together with the LOYTEC NIC software. The RNI can be utilized for remote access and configuration as well as trouble-shooting with the remote LPA.

In particular, the LINX-100's RNI appears as a regular LOYTEC network interface on the PC. The LOYTEC NIC software needs to be installed to utilize this interface also in LNS-based applications such as NL-220 or LonMaker. Using this software, the LINX-100 can act as a direct interface to its local FT channel to be managed by LNS or similar tools. For more information on how to configure the LOYTEC NIC software on the PC, please refer to the LOYTEC NIC User Manual [2].

8.2 Remote LPA Operation

The LINX-100 supports remote LPA access through its RNI. This means that a CEA-709 protocol analyzer connected to the Ethernet network can connect to the LINX-100 and record all packets on the CEA-709 channel (FT-10). The LOYTEC LPA-IP supports this advanced feature. The functionality is shown in Figure 118.

The LPA-IP runs on a Windows PC that is connected to the Ethernet network. In the NIC-IP/RNI device selection window, one can for example select the LINX-100 with IP address 192.168.1.210 and display all packets on the FT-10 channel connected to the LINX-100 with IP address 192.168.1.210. Please consult our product literature for the LPA-IP to learn more about this IP-based CEA-709 protocol analyzer.

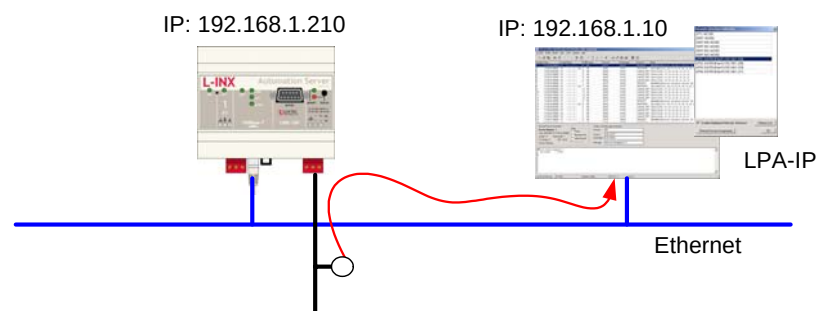


Figure 118: Remote LPA on the LINX-100.

9 OPC Server

9.1 XML-DA OPC Server

9.1.1 Access Methods

The primary function of the LINX-10X is to expose data points to the built-in OPC server. The OPC tag namespace is built from the data point hierarchy, which has been configured by the Configurator software. The OPC server on the device implements the data access standard via the Web service interface XML-DA. The OPC XML-DA Web service is accessible via the URI

<http://192.168.24.100/DA>

where the IP address has to be replaced with the actual IP address of the LINX-10X. The Web service is accessible over the same TCP port as the Web server. The default TCP port is 80. The Web server port can only be changed via the console or in the L-Config tool (see NIC User Manual [2]).

Since the Web service is easily routable on the Internet, the LINX-10X OPC server implements the basic authentication method to protect the system from unauthorized write access. Read access is available without authentication. The basic authentication involves the operator user and the password configured for this user. On how to configure the operator's password, please refer to Section 4.1. To disable the basic authentication, clear the operator's password.

<i>Note:</i>	<i>It is highly recommended to use basic authentication when exposing crucial data points over the Web service.</i>
--------------	---

To use the exposed OPC data points, there exist several possibilities:

- Use LOYTEC's L-WEB visualization tool that comes free with the LINX-10X,
- use a standard OPC client or SCADA package, or
- create your own Web service client with custom Web Pages.

The easiest way to visualize the network's data points over a Web-based interface using the LINX-10X is the L-WEB software. This software is fully integrated into the LINX-10X Configurator and allows designing graphical page content. The tool is intuitive to use like the L-VIS graphical page designer. The resulting L-WEB application is stored on the LINX-10X and can be directly accessed in your Web browser or other Internet appliances, such as PDAs. For more information on the L-WEB refer to Section 9.2.

Standard OPC clients and SCADA packages, which shall visualize the LINX-10X's data points, must conform to the OPC XML-DA standard. This means they must support the OPC Web service and not only the COM/DCOM protocol. If your SCADA package does not support OPC XML-DA, a PC-based bridge from XML-DA to the COM-based protocol can be used. The bridge software is running on a PC and translates from COM/DCOM requests into XML-DA Web service requests. The system is depicted in Figure 119.

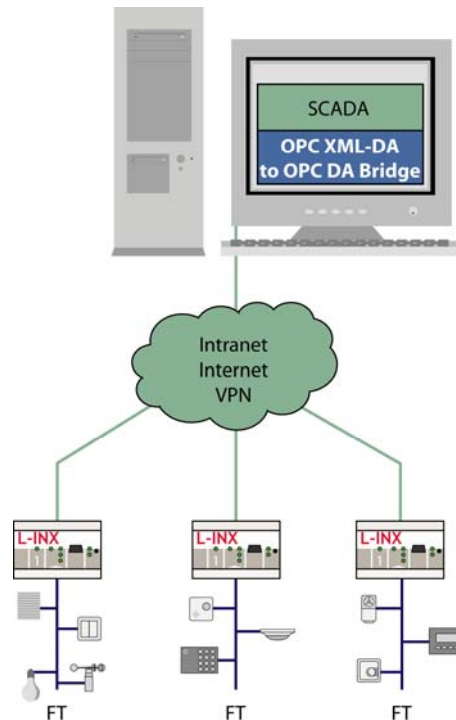


Figure 119: Using a XML-DA/DCOM bridge.

With the bridge configured to access a number of LINX-10X, the COM-based SCADA application can access a COM-based OPC server for each LINX-10X. The bridge software OPCBR-800 can be purchased and installed on any PC. This is discussed in Section 9.3.

If L-WEB is not used, customers can create their own XML-DA clients based on the WSDL for OPC XML-DA. Refer to Section 9.4 for more information.

9.1.2 Data Points

The data point hierarchy as configured by the LINX-10X Configurator software is exposed to the OPC tag namespace by the LINX-10X. This is done internally for all data points, which are marked for OPC exposure (i.e., have the OPC check-mark set).

Folders are translated into OPC nodes. Any of the data point classes, analog, binary, multi-state, string, and user, are exposed as OPC tags. Each OPC tag contains the value of the data point and some of its meta-data. An example of browsing the OPC tags on the LINX-10X is shown in Figure 120.

The OPC quality property of a given OPC tag is coupled to the data point status. If a data point is offline or unreliable, the OPC quality property changes to *uncertain*.

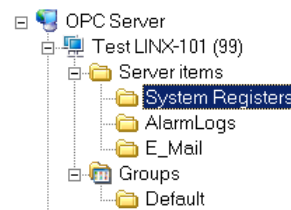


Figure 120: Client browsing the OPC tag namespace on a LINX-10X.

9.1.2.1 Analog

Analog data points are exposed as a one-to-one mapping to OPC tags. For each analog data point, an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '5' (Double).
- Item Value (Double): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.
- Item EU Type (Integer): This property is '1'.
- High EU (Double): This is the analog maximum value of the data point.
- Low EU (Double): This is the analog minimum value of the data point.
- EU Units (String): This is the human-readable engineering units text of the data point.

9.1.2.2 Binary

Binary data points are exposed as a one-to-one mapping to OPC tags. For each binary data point, an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '11' (Boolean).
- Item Value (Boolean): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.

- Contact Close Label (String): This property contains the active text of the binary data point.
- Contact Close Label (String): This property contains the inactive text of the binary data point.

9.1.2.3 Multi-state

Multi-state data points are exposed as a one-to-one mapping to OPC tags. For each multi-state data point an OPC tag is created. The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '3' (Integer).
- Item Value (Integer): The present data point value.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.
- Item EU Type (Integer): This property is '2' for multi-state.
- Enumerated EU (Array of String): This property contains the state texts of the data point.

9.1.2.4 User Type

User-type data points contain a byte array of user-defined data. Data points of user-type are also exposed as a one-to-one mapping to OPC tags. For each such data point, an OPC tag is created. The item value of the user-defined data is a hex string without whitespace representing the byte array, e.g., "B034". The OPC tag contains a number of OPC properties, which are derived from the data point's properties:

- Item Canonical Data Type (SmallInt): This property indicates the data type '8' (String).
- Item Value (String): A hex string without whitespace representing the byte array.
- Item Quality (SmallInt): The value quality. It is "good" if the data point is in normal state, or "uncertain" if the data point has an off-normal state, e.g., offline or unreliable.
- Item Timestamp (Date): This property contains the timestamp of the last value update.
- Item Access Rights (Integer): This property defines whether the tag is read-only or read/write.
- Item Description (String): This is the description of the data point.

9.1.2.5 Structured Data Points

Structured data points are modeled as one user-type data point, which contains the entire structure value as a byte array. The respective structure fields are created as sub-data points of appropriate class. For example, a SNVT_switch in CEA-709 would be modeled as one user-type data point of 2 bytes length, and two sub-data points, one an analog (value member) and one a multi-state (state member).

The relation between user-type data point and sub-data points is also exposed to OPC. In this case, an OPC node is created for the user-type data point. In that node, the sub-data points are exposed as OPC tags. The entire structure is also exposed as a user-type OPC tag under the same OPC node.

Important!

Deselect any un-used structure members from OPC exposure to reduce the number of total OPC tags.

It is important to note, that when using structured data points the top-level and all its structure members are exposed as OPC tags by default. Using many structured data points may lead to exceeding the OPC tag limit. Please observe this limit in the Configurator's statistics tab and deselect the **OPC Tag** check box for unwanted structure members. This helps to keep your configuration lean and improves the performance of the OPC server when browsing and subscribing.

9.1.3 AST Objects

The alarming, scheduling, and trending (AST) objects are more complex than regular data points. The OPC XML-DA standard does not have appropriate tags for those objects. Therefore, the LINX-10X exposes AST objects as a set of OPC tags describing the object. All tags for one AST object are collected under an OPC node representing the AST object.

9.1.3.1 Scheduler Object

The LINX-10X exposes the scheduler objects to OPC XML-DA tags. Each scheduler object is represented by a node in the OPC name space. The content of the schedule XML document referred to in this section must be compliant to the scheduleCfG schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace 'http://www.loytec.com/xsd/scheduleCfG/1.0/'.

In that node, the following OPC tags are available:

- ServiceType (string, Read-only, const): This is a constant tag of type string, which contains "schedule". It identifies this folder as a schedule folder. This can be used as an additional identification to the vendor-specific property of the folder tag.
- Schedule (string, read/write): This tag configures the schedule. The data type is string and the format is in XML. The XML document contains the *scheduleCfG* element as the root element.
- Caps (string, read-only): This tag contains the schedule capabilities. The data type is string and the format is in XML. The XML document contains the *scheduleCapabilities* element as the root element.
- CallItemPath (string, Read-only, const): This is an optional tag. If present, it contains the item path to the calendar object, that the schedule references. To read the calendar referenced by the schedule, use this item path and the "Calendar" item name to read the calendar XML document.
- EmbeddedCal (node): This is an optional OPC node. If present, it contains the OPC tags for the embedded calendar. The embedded calendar structure is as defined for calendar objects in Section 9.1.3.2.

9.1.3.2 Calendar Object

The LINX-10X exposes the calendar objects to OPC XML-DA tags. Each calendar object is represented by a folder in the OPC name space. In that folder, the following OPC tags shall be available:

- **ServiceType** (string, Read-only, const): This is a constant tag of type string, which contains “calendar”. It identifies this folder as a calendar folder. This can be used as an additional identification to the vendor-specific property of the folder tag.
- **Calendar** (string, read/write): This tag configures the calendar. The data type is string and the format is in XML. This document contains the *calendarCfg* element as the root element.
- **Caps** (string, read-only): This tag contains the calendar capabilities. The data type is string and the format is in XML. The XML document contains the *calendarCapabilities* element as the root element.

9.1.3.3 Alarm Objects

The LINX-10X alarm objects provide the *alarm summary* and can be used to acknowledge alarms. The alarm objects are exposed to XML-DA tags. Each alarm is uniquely identified by an XML alarm ID (XAID). The XAID must identify the alarm object and the alarm ID in that object. The XAID is used in the acknowledge service to identify the alarm. The XAID can also be transmitted in e-mail notifications.

Each alarm object is represented by a folder in the OPC name space. In that folder, the following OPC tags shall be available:

- **ServiceType** (string, Read-only, const): This is a constant tag of type string, which contains “alarm”. It identifies this folder as an alarm folder. This can be used as an additional identification to the vendor-specific property of the folder tag.
- **Summary** (string, Read-only): Reading from this tag, the current alarm summary can be obtained. The data type is string and the tag contains an XML document. This tag should not be subscribed to as it contains a large document. Subscribe to *NotifyCnt* instead, to get notified about new alarms. The root element of the XML document is the *alarmSummary* element.
- **NotifyCnt** (unsigned, Read-only): This tag is updated with an incremented notify count for each alarm update notification. This is the case for new or cleared alarm conditions, and for acknowledged alarms. Clients can subscribe to this tag in order to be notified about changes in the alarm summary. The client has then to read the complete alarm summary when notifications occur.
- **Ack** (string, Write): Writing to this tag acknowledges an alarm. The data type is string. The written data is an XML document, which contains the *alarmAck* element. The write must specify the XAID.

9.1.3.4 Trend Log Objects

Each trend log object on the LINX-10X is represented by a folder in the OPC name space. This folder contains a number of tags describing and controlling the trend log. To retrieve log records however, the XML-DA tag interface cannot be used. There are two options: retrieve the complete log as a CSV file, or use the LOYTEC proprietary Data Log Web service (XML-DL). That Web service uses the *logHandle* provided by a tag. The CSV file location can be obtained from a tag also.

- **ServiceType** (string, Read-only, const): This is a constant tag of type string, which contains “trendLog”, or “alarmLog”. It identifies this folder as a trend log, data log or

alarm log folder. This can be used as an additional identification to the vendor-specific property of the node tag.

- **Purge** (Boolean, read/write): When writing TRUE to this tag, the log is purged.
- **TotalCnt** (unsignedInt, read-only): This tag contains the total number of logged records. This number can be larger than the BufferSize.
- **BufferSize** (unsignedInt, read/write): The size in records of the log buffer. Writing to this tag can resize the log buffer, if it is disabled.
- **LogHandle** (string, read-only, const): This handle specifies the data log. The logHandle must be used with the proprietary Data Log Web service.
- **CsvFile** (string, read-only, const): This tag specifies the file path and file name of the CSV data log file.
- **CentralDL0, CentralDL1** (string, read/write): These tags serve as placeholders for the central data logger to store its URI. The tag CentralDL0 is intended for the primary, CentralDL1 for the secondary central data logger. The tags are stores in non-volatile memory and retain their values over a power-on reset. For more information on the central data logger refer to LWEB-801 User Manual [4].

9.1.3.5 E-mail Templates

E-mail templates can be configured in the LINX-10X Configurator software. When an e-mail template is triggered, the corresponding e-mail is transmitted. The e-mail template can also be triggered over the OPC interface. Therefore, a node is added to the OPC name space for each e-mail template under the “E_Mail” node.

Each e-mail node is named after the e-mail template and contains the following OPC tags:

- **ServiceType** (string, Read-only, const): This is a constant tag of type string, which contains “email”. It identifies this folder as an e-mail template folder.
- **Send** (Boolean, read/write): When writing TRUE to this tag, the e-mail transmission is triggered.

9.2 Using L-WEB

The L-WEB is a Web-based visualization software that comes free with the LINX-10X. It uses the standard Web technologies to visualize and control data provided by one or more LINX-10X or LINX-20X Automation Servers on a Windows PC.

The L-WEB software uses the standardized OPC XML-DA Web service to communicate between L-WEB and remote LINX-10X or LINX-20X Automation Servers, which makes it extremely firewall-friendly and easy to setup.

The graphical design of the L-WEB user interface consists of pages, which can simply be created by using the L-VIS/L-WEB Configurator software without any know-how in HTML, Java, etc. Dynamic information is shown in the form of numeric values, text, changing icons, bar graphs, trend logs, alarm and event lists, or schedule controls.

The complete set of automation functions of the LINX-10X or LINX-20X Automation Server is fully supported by L-WEB. The automation services are residing in the embedded LINX-10X or LINX-20X Automation Servers and distributed over the network to build up a dependable system with L-WEB only accessing these services. Furthermore, any kind of calculations, data point connections, etc., are implemented on the embedded Automation

Server, which makes the application on the Automation Server completely independent from the connection to the L-WEB application.

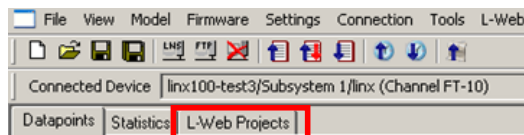
Starting from the LINX-10X data point configuration, the user can create an L-WEB project. The L-WEB project contains the data point configuration of the Web service interface and a graphical design for the L-WEB user interface. For more information on creating graphical designs using the L-VIS/L-WEB Configurator software refer to the L-VIS User Manual [5].

9.2.1 Create a new L-WEB Project

The LINX-10X Configurator provides the data point configuration, which is downloaded to the device. On top of that configuration, an L-WEB design can be created for visualization.

To Create an L-WEB Project

1. Start the Configurator software and change to the **L-WEB Projects** tab.



2. The L-WEB project tab appears as in Figure 121.

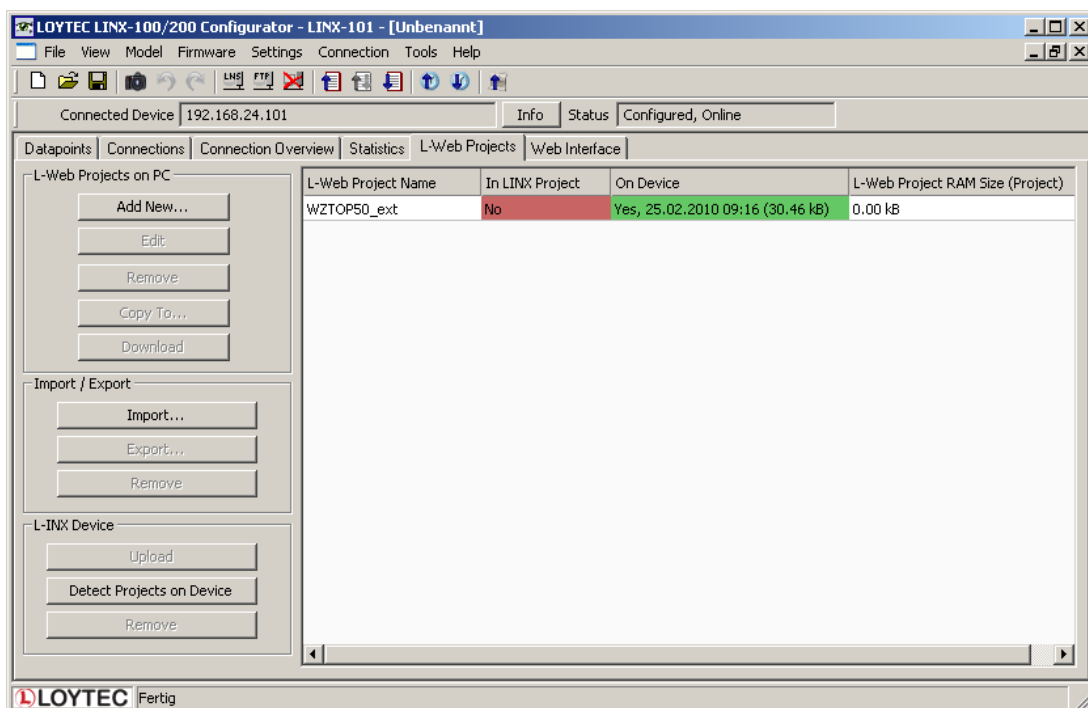
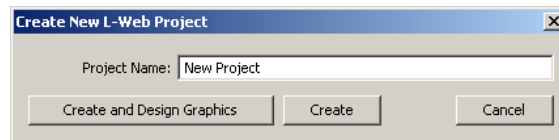


Figure 121: L-WEB Projects Tab.

3. Click on **Add New ...**
4. Enter a new **Project Name**.



- Click on **Create**. The new project appears in the projects list.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	No	No	0.00 kB

9.2.2 Start a Graphical L-WEB Design

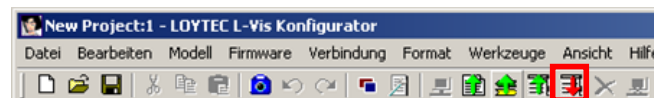
The L-WEB graphical design tool is started from within the L-WEB projects tab. The graphical design for the L-WEB project is created in the L-VIS design tool. The data point configuration created in the LINX-10X configuration project is available for the L-WEB project and its graphical design.

To Start a Graphical Design

- Select the **L-WEB Projects** tab.
- Select an L-WEB project.
- Click **Edit**.



- This opens the L-VIS graphical design tool. Complete the graphical design in the tool and click the **Write Project to Device** speed button



- The graphical design is now part of the project.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	Yes, 26.02.2010 17:01 (5.32 kB)	No	57.17 kB

Note: If the Configurator had been connected to the device, the graphical design would have been added to the device in the same step.

9.2.3 Organize L-WEB Projects

L-WEB projects can be organized within the LINX-10X configuration project. L-WEB projects can be part of the configuration project and/or stored on the device. For instance, the configuration project may contain a number of L-WEB projects, but for saving space on the device, only one of them is downloaded on the device. The **L-WEB projects** tab provides a number of tools to organize a set of L-WEB projects.

To Organize L-WEB Projects

- Connect to the device as described in Section 6.7.2.
- Select the **L-WEB Projects** tab.
- Click **Detect Projects on Device**. This scans for all projects found on the device.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	Yes, 28.02.2010 17:01 (5.32 kB)	No	57.17 kB
Second Project	Yes, 28.02.2010 17:03 (5.31 kB)	Yes, 28.02.2010 16:03 (5.31 kB)	57.18 kB

Projects marked as a green **Yes** in the **In LINX Project** column are L-WEB projects, which are part of the current LINX-10X configuration project. Projects marked as a green **Yes** in the **On Device** column are L-WEB projects, which are also stored on the device. A red **No** identifies the L-WEB project to be missing in the project or on the device, respectively.

- If you want to download an L-WEB project to the device, which is missing there, select the project and click **Download**. After the download the project appears with a green **Yes** in **On Device**.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	Yes, 28.02.2010 17:06 (5.32 kB)	Yes, 28.02.2010 16:06 (5.32 kB)	57.17 kB
Second Project	Yes, 28.02.2010 17:07 (5.31 kB)	Yes, 28.02.2010 16:07 (5.31 kB)	57.18 kB

- If you want to remove a project from the device, click **Remove** in the **LINX Device** box.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	Yes, 28.02.2010 17:06 (5.32 kB)	Yes, 28.02.2010 16:06 (5.32 kB)	57.17 kB
Second Project	Yes, 28.02.2010 17:03 (5.31 kB)	No	57.18 kB

- If you want to remove the project from the current LINX-10X project file, click **Remove** in the **L-WEB Projects on PC** box.

L-Web Project Name	In LINX Project	On Device	L-Web Project RAM Size (Project)
New Project	Yes, 28.02.2010 17:06 (5.32 kB)	Yes, 28.02.2010 16:06 (5.32 kB)	57.17 kB
Second Project	No	No	0.00 kB

- If you want to export the L-WEB project into a separate L-WEB project file, click **Export...** and select a file name in the file requestor dialog.
- If you want to import an L-WEB project from a separate L-WEB project file, click **Import...** and select the file in the file requestor dialog. The L-WEB project appears in the project but not on the device.

9.3 Using the OPC Bridge

9.3.1 Software Installation

The LOYTEC OPC Bridge software LOPC-BR800 is installed as a separate application on a PC. A license for the LOYTEC OPC Bridge software must be purchased separately. With one software license for the OPC Bridge, multiple LINX-10X devices can be accessed. With the OPC Bridge software installed, each configured LOYTEC LINX-10X device appears as a separate COM/DCOM server. The OPC Bridge software can be used with LOYTEC L-INX OPC servers only. The bridge won't connect to third-party OPC servers.

System requirements:

- Windows 2000, Windows XP, Windows 2003 Server, or Windows Vista.

The OPC Bridge software is available on the LOYTEC Software CD or via download from the LOYTEC Web site www.loytec.com. For installing the software, a registration code must be purchased.

To Install the OPC Bridge

1. Double click on 'lopc-br800_1_0_setup.exe' and follow the installation steps.
2. When asked, type in the bridge's registration code. Click **Next**.
3. Finalize all remaining installation steps by clicking **Next** and **Finish**.

When the installation is complete, the OPC Bridge software is available under **Programs** → **LOYTEC OPC Bridge**.

9.3.2 Configure the Bridge Locally

If the bridge software is installed on the same PC where the LINX-10X Configurator software is used to configure the LINX-10X OPC server, the server information can be automatically made available as a COM OPC server. This is done when the LINX-10X configuration is downloaded into the device.

To Configure the Bridge Locally

1. Open the Configurator software and configure the LINX-10X as described in Section 6.7.
2. In the LINX-10X Configurator menu go to **Settings** → **Project settings ...**. This opens the project settings dialog on the tab **General** as shown in Figure 122.

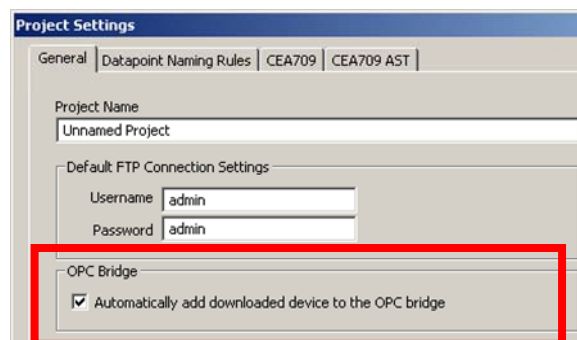


Figure 122: Enable bridge export in the project settings.

3. Put a check mark on **Automatically add downloaded device to the OPC bridge**.
4. Click **OK**.
5. Downloading the configuration also makes the LINX-10X available as a COM OPC server through the local bridge.

9.3.3 Export OPC Servers for another PC

If the bridge software is not installed locally on the same PC where the LINX-10X configuration is created, it must be exported to make the OPC server information available. The exported file can then be transferred to the OPC bridge.

To Export the Bridge Configuration

1. Open the LINX-10X Configurator.
2. Connect to the LINX-10X, which shall be available in the bridge.

3. Select the menu **File → Export to OPC Bridge Configuration....**
4. In the **OPC Bridge Device Properties** dialog as shown in Figure 123, add information which is not default, i.e., Min update rate, Wait time and Hold Time (see Section 9.3.6). If the operator user has a non-default password, enter the password.
5. Click **Export to File**.

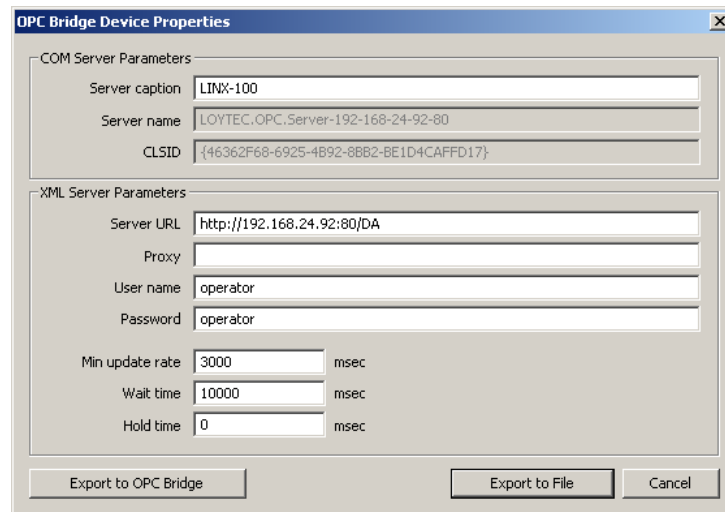


Figure 123: Bridge Export dialog.

9.3.4 Import OPC Servers Using the Configurator

When using OPC server information exported by the Configurator, the exported server definition must be imported to the OPC bridge. This can also be done using the Configurator software. The Configurator software must be installed on the same PC as the OPC bridge for doing so.

To Import a Server Definition

1. Open the Configurator software.
2. Select the menu **File → Import OPC Bridge Configuration....**
3. In the file requestor select the bridge configuration XML file, which has previously been exported and click **OK**.
4. The **OPC Bridge Device Properties** dialog displays the imported bridge information.
5. Click **Export to Bridge** to add the respective COM server to the bridge.
6. Click **Save**.

9.3.5 Manually Configure Servers

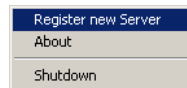
The OPC bridge configuration can also be edited manually. The same procedure is also applicable to verify imported OPC server definitions in the bridge software. After adding a server definition in the bridge software, the LINX-10X will be available as a COM OPC server through the bridge.

To Configure a Server in the Bridge

1. Start the OPC bridge from the Windows Start menu under **Programs → LOYTEC OPC Bridge → OPC Bridge manual Setup**.

2. In the system tray, right-click on the bridge icon .

3. In the context menu select **Register new Server**.



4. In the **Register Server** dialog click **Add**.
5. A new server entry is added. Enter the information on **Server caption** (this is displayed), **Server name** (this is the COM object name), and the **Server URL** (the URL of the LINX-10X device) as shown in Figure 124.

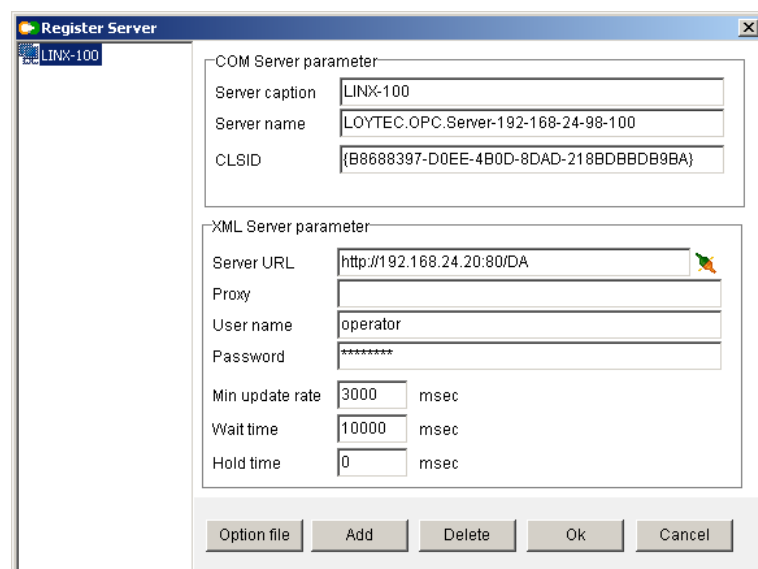


Figure 124: Register Server dialog in the bridge software.

6. Additionally, enter the 'operator' as the **User name** and its **Password** on the device. Enter the default timing parameters (min update rate 3 sec, wait time 10 sec, hold time 0). For information on the timing parameters refer to Section 9.3.6.
7. To test the connection to the LINX press the button .
8. Click **OK**.

9.3.6 Bridge Timing Parameters

The OPC bridge uses three timing parameters to operate on the OPC XML-DA side. The defaults for those parameters are good for most cases. For specific use cases, however, they might need to be adapted.

- **Minimum Update Rate:** This parameter defines the rate at which the LINX server will update its value caches. In general value changes could occur much more frequently than the value caches are updated. Therefore, the minimum update rate determines the granularity at which updates may be notified to the OPC client. If an OPC client specifies an update rate less than this value for a group of subscribed data

points, the group will not be updated faster. If the group specifies a slower update rate, however, the LINX will be polled less often. Lowering this parameter gives better responsiveness to data changes but also increases the XML-DA traffic and impacts overall performance. The recommended default is 3 seconds.

- **Wait Time:** This parameter specifies how long the OPC bridge shall wait for value updates before issuing the next polled refresh to the LINX. This time can be higher than the update rate because changes are notified within the wait time as soon as they occur on the LINX. The recommended default is 10 seconds.
- **Hold Time:** This parameter specifies that changes will be held back by the LINX for the given amount of time before they are notified to the client. Normally, changes in the LINX are notified at the update rate's granularity. In rare cases this can be used to hold back changes beyond the update rate. The recommended default is 0.

9.4 Using Custom Web Pages

Custom Web pages can also be developed for the LINX-10X. For doing so, the applications engineer must implement an OPC XML-DA Web service client, which adheres to the WSDL interface. This can be done in C++ or scripting languages such as Perl. The WSDL must be obtained from the OPC Foundation's Web site following the OPC XML-DA namespace <http://opcfoundation.org/webservices/xmla/1.0/>.

Any Web content, including scripts, applications or static Web pages can be stored directly on the LINX-10X's file system. Use the admin account to upload the content via FTP into the directory

`/var/www`

For example, a page named 'my_page.html' put directly into '/var/www' can be accessed via 'http://192.168.24.100/my_page.html', given that the IP address is correct.

10 M-Bus

10.1 Introduction

The M-Bus (Meter-Bus) is a European standard (EN 13757-2, EN 13757-3) designed for remote reading of meters. With its standardization as a galvanic interface for remote readout of heat, water, and energy meters, this bus has become an important interface for automatic meter reading applications with different vendor's meters on the same cable.

The M-Bus is a serial bus, which is controlled by a single bus master. This master can request data from several slave devices connected to the network. The data transmission from master to slave is done by a modulation of the output voltage (36 V means a logical '1', 24 V means logical '0'). During data transmission from slave to master the current is modulated (1.5 mA represent the logical '1', 11-20 mA represent a logical '0'). M-bus devices can be powered over the bus. The number of devices which can be powered depends on the M-Bus transceiver used.

10.2 Hardware Installation

For using the M-Bus with the device an external M-bus interface with an RS-232 connector is required. The external interface must be connected to the serial console connector.

The M-Bus functionality must be enabled on the device itself. This is done by setting DIP-switch 7 to ON. This disables the console of the device and activates M-Bus over the console connector. After the device is rebooted, the M-Bus is active on the device. When rebooting the device with M-Bus activated and the console connected, a couple of boot messages are displayed in the console, before the console is turned off.

If the console is needed again, set the DIP switch 7 to OFF and reboot the device. This is required, if the firmware shall be updated over the serial port using the LSU tool.

10.3 M-Bus Network

The M-Bus network utilizes a two-wire connection. Several M-Bus slave devices are connected in parallel to the transmission medium. Each M-bus device has a primary address in the range from 0 to 250. This primary address must be unique for each device. Also a secondary address can be used for the slave devices. The secondary addressing mode is currently not supported by the LOYTEC device. The M-Bus network also supports two kinds of broadcast messages. A broadcast to address 255 does not force the slaves to give a response. A broadcast to address 254 forces an answer from the slave. This broadcast message is mainly used for peer-to-peer connections.

The M-Bus allows the use of devices with different Baud rates of up to 9600 baud. M-Bus devices are not always able to fulfill the complete functional specification of the M-Bus standard. For readout two different modes are known (some slave devices implement both):

- A default read usually reads all the data of a device.
- A selective read selects the data points, which are to be read.

Some devices also support writing special data points.

Some M-Bus devices support a synchronized action. This means that when a device receives such a synchronize command, it stores specific data points for later readout. This way, specific information of even a larger number of devices can be read out in a synchronized manner.

M-Bus supports network management functions such as changing the primary address of a device, changing the Baud rate of a device, reading all data from a device as well as pinging a device. It is therefore possible to scan M-Bus devices in an M-Bus network.

M-Bus data points are specified by a DIF/DIFE and VIF/VIFE combination. The DIF/DIFE (data information field and data information field extension) specify storage number, tariff, subunit as well as the data coding (BCD, int, etc.) and the function (min, max, etc.) of the data point. The DIF/DIFE can be up to 11 bytes long (1 byte for the DIF and up to 10 extensions). The VIF/VIFE combination (value information field and value information field extension) specifies the type of the data point (e.g. energy count value) and how it is presented (e.g., the value is given in “Wh”). Like the DIF/DIFE, the VIF/VIFE can consist of one VIF and up to 10 VIF extensions. The Configurator allows the configuration by either entering the DIF/DIFE combination or by specifying the appropriate numbers.

10.4 Web Interface

This section describes the Web interface for the M-Bus port.

10.4.1 Configuration

A configuration of the M-Bus port is not necessary, as no parameters are required for the M-Bus.

10.4.2 Data Points

M-Bus data points can be accessed through the Web UI as described in Section 4.2.11.

10.4.3 Statistics

Figure 125 shows a typical output of the statistics information which can be displayed for the M-Bus port.

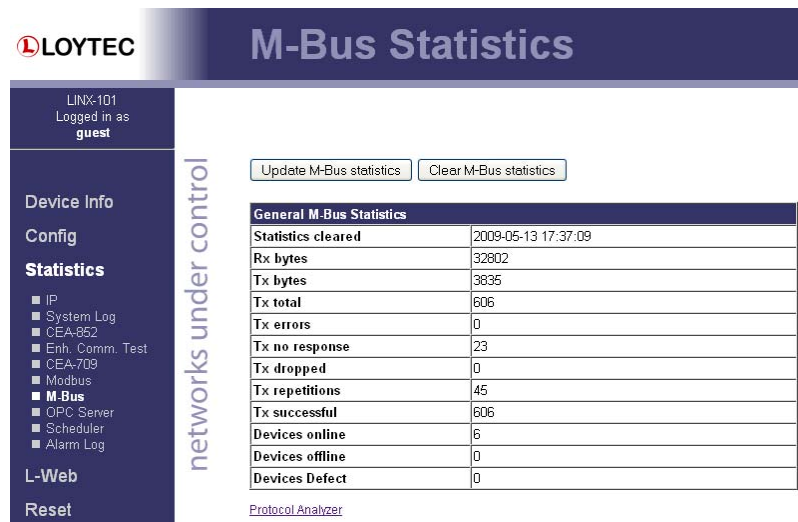


Figure 125: Statistics of the M-Bus port.

The following information is available:

- Rx bytes: number of bytes received
- Tx bytes: number of bytes sent
- Tx total: total number of transmissions
- Tx errors: number of errors during a transmission
- Tx no response: number of transmissions without a response
- Tx dropped: number of dropped transmissions (in case of an error, device responses or transmissions can be dropped)
- Tx repetitions: number repeated messages
- Tx successful: number of successful transmissions
- Devices online: number of devices which are currently online

10.4.4 M-Bus Protocol Analyzer

By activating the link Protocol Analyzer (available in all M-Bus statistics tabs), the protocol analyzer page is shown as displayed in Figure 126.

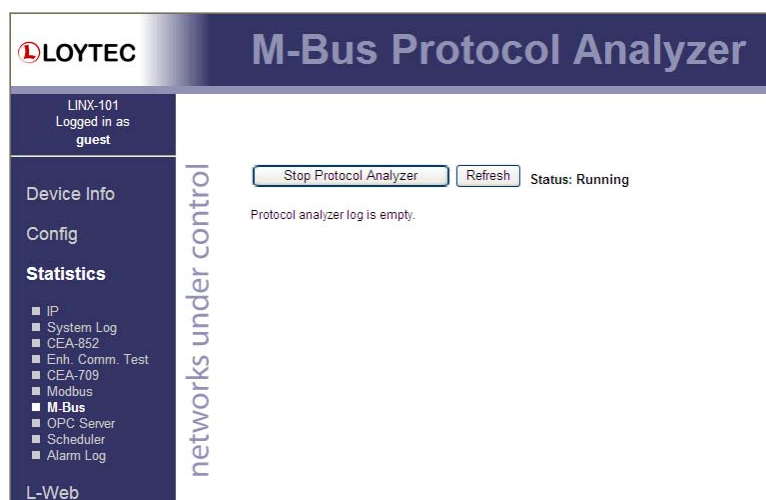


Figure 126 M-Bus protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values.

10.5 Configurator

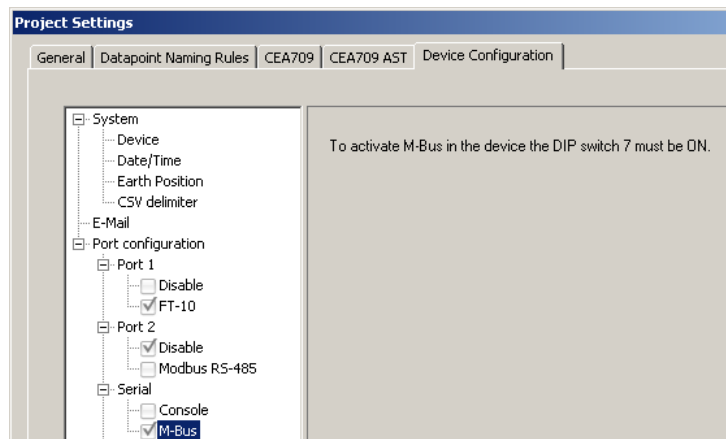
This section describes how to use the Configurator software for the management of M-Bus data points. For further information on the Configurator software refer to Chapter 6.

10.5.1 Activating M-Bus Configuration

Before a new M-Bus configuration can be managed, the M-Bus option must be enabled. The project settings are described in detail in section 6.3.

To Activate the M-Bus Configuration

1. Open the project settings dialog.
2. In the **Device Configuration** tab enable the M-Bus check box.
3. Press the **OK** button.



Important: *If the M-Bus Port is deactivated via the checkbox or a firmware or model version is chosen, which does not support M-Bus, the complete M-Bus configuration is deleted. In this case a dialog is displayed, which has to be confirmed.*

10.5.2 Data Point Manager for M-Bus

The Configurator uses a central concept to manage data points. The data point manager as shown in Figure 127 is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (Figure 127),
- The data point list (Figure 128),
- And a property view.

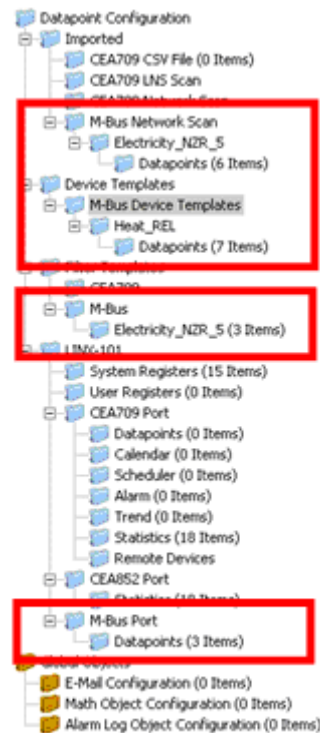


Figure 127: Data Point Manager Dialog with M-Bus folder list.

No. ▲	OPC	Direction		Datapoint Name	M-Bus Counter Type	Storage	Tariff	Subunit	Function	Device Address	ID
19	☒	In		Electricity_JAN_4_Operating Time1	Operating Time	0	0	2	instVal	4	1055
20	☒	In		Electricity_JAN_4_Operating Time2	Operating Time	0	0	3	instVal	4	1056
21	☒	In		Electricity_JAN_4_Operating Time3	Operating Time	0	0	4	instVal	4	1057
22	☒	In		Electricity_JAN_4_Operating Time4	Operating Time	0	0	5	instVal	4	1058
23	☒	In		Electricity_JAN_4_Operating Time5	Operating Time	0	0	6	instVal	4	1059
24	☒	In		Electricity_JAN_4_Operating Time6	Operating Time	0	0	0	instVal	4	105A
25	☒	In		Electricity_JAN_4_Current	Current	0	0	4	instVal	4	105B
26	☒	In		Electricity_JAN_4_Power	Power	0	0	5	instVal	4	105C
27	☒	In		Electricity_JAN_4_Power1	Power	0	0	6	instVal	4	105D
28	☒	In		Electricity_JAN_4_Power2	Power	0	0	7	instVal	4	105E

Figure 128: Datapoint Manager Dialog with M-Bus Data Point List.

10.5.3 Folder List

At the left is a list of folders which is used to sort the available data objects by their category. There are a number of predefined M-Bus folders available. All other folders are described in section 6.2.1:

- **Imported:** This folder has a number of sub-folders for different import methods:
 - **M-Bus Network Scan:** This folder holds data points scanned online from an attached M-Bus network. When scanning an M-Bus device, a subfolder is created under M-Bus Network Scan. The name of this subfolder is generated automatically from the information of the scanned device. Additionally under the device sub-folder a data point folder is created.

Data objects in the import folder are not stored on the device when the project is downloaded. They represent data objects, which are available on remote devices and are shown here as templates to create suitable data objects for use on the device by selecting the **Use on Device** option.

- **Device Templates:** This folder contains created data point templates for the different technologies.

- **M-Bus Device Templates:** This folder contains a sub-folder for each device, which is imported from an M-Bus device template. This device folder also contains a sub-folder with the data points specified in the template. Data points can be added to the folder. Additionally suitable data objects can be created for the use on the device by selecting the **Use on Device** option.
- **Filter templates:** This folder contains filter templates for scanned M-Bus devices
 - **M-Bus:** This folder contains a folder with data points for each created filter template.
- **LINX-10X:** This is the device folder of the LINX-10X. It contains all the necessary data points which constitute to the LINX-10X's port interface definition. These data points are created on the LINX-10X when the configuration is downloaded. For M-Bus an additional sub-folder exists:
 - **M-Bus Port:** This folder contains the remote M-Bus data points, which are used on the device.

Using the context menu on a folder, sub-folders may be created to organize the available objects. If new objects are created automatically, they are usually placed in the base folder and can then be moved by the user to any of his sub-folders. Note, that the folder structure described above cannot be changed by adding or deleting folders at that level.

10.5.4 Network Port Folders

The M-Bus network port folder on the device has the same structure of sub-folders as the other network port folders in Section 6.2.2. Currently only the **Datapoints** folder exists for the M-Bus network port.

10.5.5 M-Bus Properties

Apart from the common data point properties discussed in Section 6.2.4 the data points of the M-Bus technology have additional properties:

- **Storage Number:** This property defines the M-Bus storage number of the data point. This number can also be specified by the manufacturer using a DIF/DIFE combination.
- **Tariff:** This property defines the tariff of the M-Bus data point. This number can also be specified by the manufacturer using a DIF/DIFE combination.
- **Subunit:** This property defines the subunit of the M-Bus data point. This number can also be specified by the manufacturer using a DIF/DIFE combination.
- **Function Field:** This property defines the function field of the M-Bus data point. Possible values for this property are instantaneous value, maximum value, minimum value and value during error state. This number can also be specified by the manufacturer using a DIF/DIFE combination.
- **Data Coding:** This property defines how the value for this data point is coded. The information is not relevant for input data points but it is mandatory for output data points. Possible values for this property are instantaneous value, maximum value, minimum value and value during error state. This number can also be specified by the manufacturer using a DIF/DIFE combination.
- **VIF/VIFE:** The VIF and VIFE (Value Information Field and VIF Extension) specify the counter type and its scaling. When the most significant bit of a VIF or VIFE is set, another VIFE follows. Up to ten VIFEs can be specified. When this combination is entered, also the M-Bus counter type and the unit are updated according to the VIF/VIFE combination.
- **M-Bus Counter type:** This information is derived from VIF/VIFE. It informs about the type of the data point value (e.g. Energy counter value or operating time).

- **M-Bus Device Name:** This property shows the name of the M-Bus device the remote data point is connected to.
- **M-Bus Device Address:** This property shows the address name of the M-Bus device the remote data point is connected to.
- **Pollgroup:** Each M-Bus input data point is attached to a poll group. If more than one poll group is available, the poll group can be selected. This property is not shown for output data points.

10.5.6 M-Bus Workflow

This section discusses the workflows for setting up an M-Bus environment. The network can either be set up online using the network scan function or also offline by either setting up the devices and data points manually or by using M-Bus device templates. The change of primary addresses and Baud rates can only be done online.

10.5.6.1 Offline Engineering

This section describes how an M-Bus network can be set up without using the M-Bus network. Figure 129 shows the workflow. First the address and Baud rates of the M-Bus devices must be configured for example by following the device manufacturer's guidelines. Afterwards the devices and data points are configured in the Configurator either configured manually or by using M-Bus device templates. Also mixing the two methods is possible. When using the device templates also data points can be added manually. The configuration is then downloaded to the device and the device is rebooted.

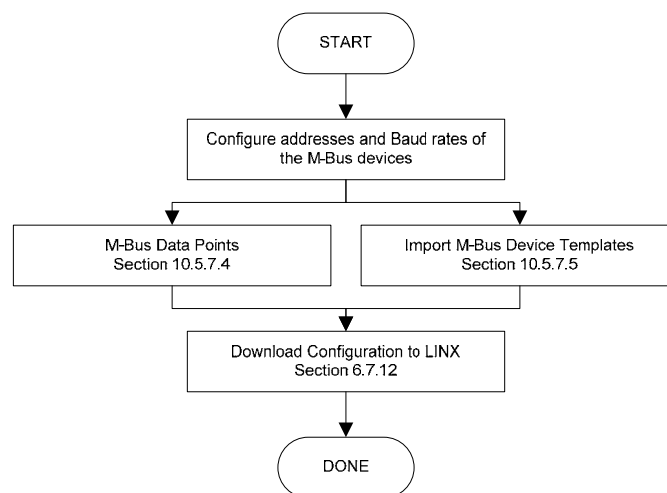


Figure 129: Workflow for offline engineering.

10.5.6.2 Online Engineering

This section describes how the M-Bus network is set up when the network can be accessed. Figure 130 shows the workflow. If necessary the addresses and baud rates the M-Bus devices are using can be configured using the Configurator. The devices and data points can then be configured by scanning the connected devices, manual configuration or also by using the M-Bus device templates.

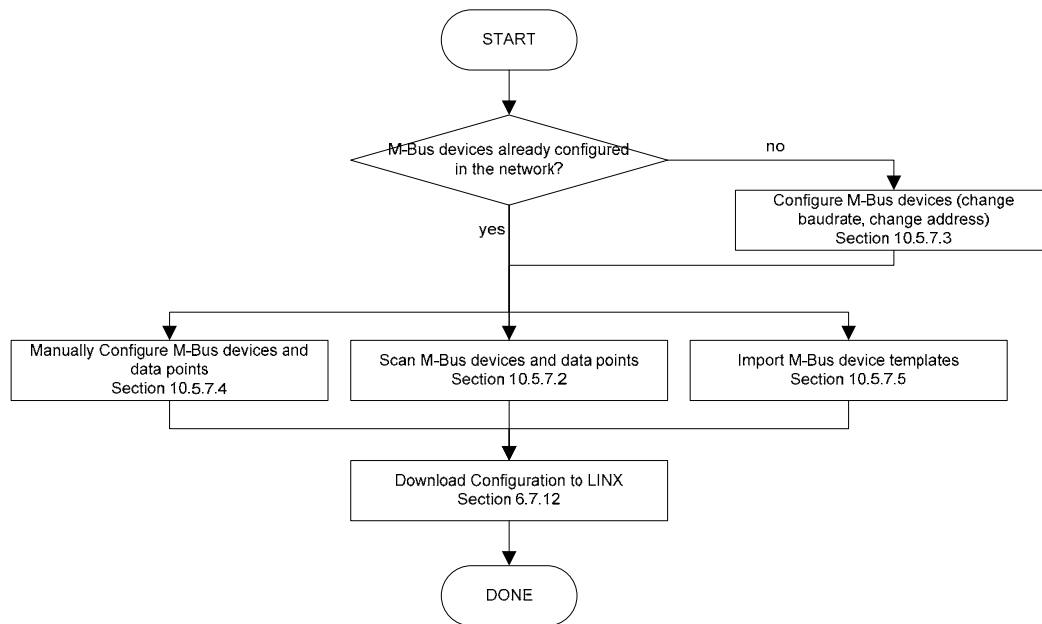


Figure 130: Workflow for online engineering.

10.5.7 Using the Configurator for M-Bus

10.5.7.1 Automatic Naming

Operations which automatically generate M-Bus data points or allocate M-Bus devices use auto naming. Automatic naming is also used, when a device is applied and no device name is specified.

The automatic device name is concatenated from the device medium (e.g. Electricity), the 3 character M-Bus manufacturer code and the address. For example the device could be automatically named “Electricity_LOY_7”. If a name is specified, the device name of the applied device is concatenated the address, e.g. “Device_7”.

The automatic data point name is concatenated from the device name the data point is related with and the type of the data point. For example if a data point is an energy counter value in the device “Electricity_LOY_7”, the name “Electricity_LOY_7_Energy” is created.

10.5.7.2 Scanning the M-Bus Network

The Configurator software can connect to the device and perform an M-Bus network scan. The network scan searches for connected M-Bus devices and data points on those devices. The device scan goes through each address on the M-Bus network using the specified baud rates. When scanning for a device the M-Bus scanner starts with the highest specified baud rate. If the device is found, it is added to the device list, if not, the scan tries to find the device address with the next lower baud rate and so on.

The M-Bus scan can only scan for input data points. Output data points can be created manually or imported via a device template.

To Scan for Devices

1. Connect to the device via FTP as described in Section 6.7.2.
2. Right click on the Folder **M-Bus Network Scan** and select **Scan M-Bus Network**. This opens the **M-Bus Network Scan** Dialog shown in Figure 131.

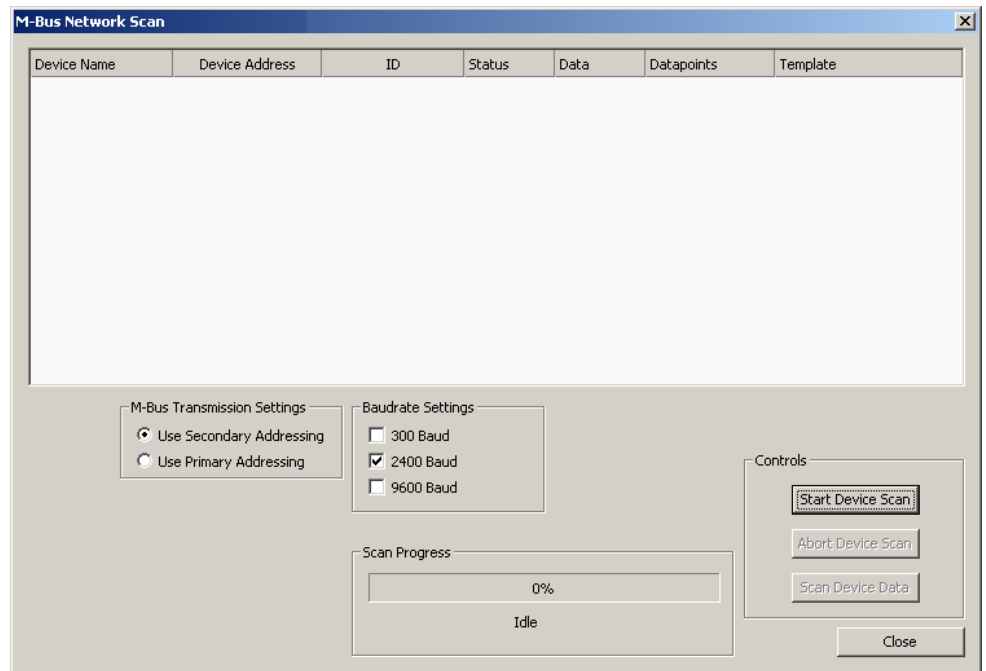
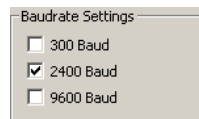


Figure 131 M-Bus Network Scan dialog.

3. In **M-Bus Transmission Settings** choose the address scanning mode. The default is secondary address scanning. This prevents problems with duplicate primary addresses of previously uninstalled M-Bus devices.
4. Select all applicable baud rates for the device scan.

**Important:**

Selecting 300 baud results in a very slow scan. Aborting the scan is possible using the Abort Device Scan button.

5. Start the scan by pressing the **Start Device Scan** button. The progress bar shows the progress of the scan. Under the progress bar, a text displays, which device is currently scanned. When a device is found, it is displayed in the device list. The name of the device is automatically created as described in section 10.5.7.1.
6. The scan can be aborted by selecting the **Abort Device Scan** button.
7. When the device scan is finished (either aborted or ended), the devices can be selected for a data scan. Also multi-select is possible.
8. Select the devices which have to be scanned for data points and press the **Scan Device Data** button. This scans all data points of the selected devices. For every device a folder with the name of the device is created under the **M-Bus Network Scan** folder. The data points found are placed in the **Datapoints** folder of the appropriate devices.

To Use Datapoints from a Scan

1. Go to the **Datapoints** folder of the device of the M-Bus scan.
2. Select the desired data points, also multi-select is possible.

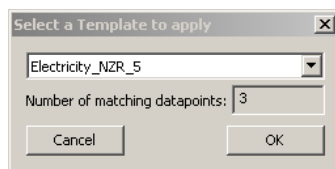
3. Either press on the **Use on Device** button  or right-click and select **Use on Device**. The selected data points are now available in the **Datapoints** subfolder of the **M-Bus Port** folder.

To Create Filter Templates from a Network Scan

1. Go to the **Datapoints** folder of the device of the M-Bus scan.
2. Select the desired data points, you wish to create a template from, also multi-select is possible.
3. Right click on one of the selected data points and select **Use as Template**. This creates a folder, containing the selected data points.

To Use data points from a Scan using Filter Templates

1. Right click on the folder M-Bus Network Scan and select either **Use on device and apply single M-Bus filter templates** or select **Use on device and apply all M-Bus filter templates**. When all filter templates are applied, all matching data points from the scan are used on the M-Bus port of the device.
2. When **Use on device and apply single M-Bus filter templates** is selected, the following dialog is opened:



3. The drop down box shows all available M-Bus filter templates. As additional information, when a filter template is chosen, the number of data points is displayed, which match the template.
4. Select **OK** to use the data points on the device.

10.5.7.3 Network Management Functions

This section describes how the M-Bus network management functions can be used. It describes adding and removing M-Bus devices as well as changing the baud rate or the primary address. The tasks can be performed offline as well as online.

The **Network Management** dialog shown in Figure 132 shows a list of devices. Devices which have been scanned using a network scan have the status online, devices which have been created manually or using device templates have the status offline. If a device which is online also has been scanned for device data, a green checkmark is displayed in the **Data** column.

To Start the M-Bus Network Management Dialog

1. Connect to the device via FTP as described in section 6.7.2.
2. Select the M-Bus dialog by clicking on the **M-Bus** button



in the tool bar of the **Datapoints** tab. The M-Bus Management dialog opens, showing the **Network Management** tab displayed in Figure 132.

Device List

Device Name	Device Address	Status	Data	Datapoints	Template
Other_REL_2	2	online	✖	0	
Heat_REL_1	1	online	✖	0	
Electricity_NZR_5_1	5	online	✓	6	
Water_INW_6	6	online	✖	0	
Electricity_JAN_4	4	online	✖	0	
Water_SEN_7	7	online	✖	0	

Device Properties

Device Name:

Device Address: ... [0 ... 255]

Device Baud rate:

Optional Device Information

Manufacturer ID:

Version: [0 ... 255]

Medium:

Model Name:

Network Scan

☐ 300 Baud ☐ 2400 Baud ☐ 9600 Baud

☒ 2400 Baud

Progress:

Device Capabilities

☐ Default Read ☐ Selective Read

Controls

Figure 132: M-Bus network management dialog.

To Add an M-Bus Device Manually Without Scanning

1. Fill in the **Device Address** and select a **Device Baudrate** from the drop down box.
2. A **Device Name** can be specified. If more devices with the same properties have to be created using subsequent addresses, the end address can be specified in the input field on the right hand side of the **Device Address** field.

Device Address ... [0 ... 255]

3. The device capabilities specify, what kind of M-Bus read requests the device is able to process. If nothing is specified here, **Default Read** is used. Default read usually means that the M-Bus device transfers all its data during a read. Selective read means that the data point which is to be read can be selected during the read request. If the device is able to perform such a request, **Selective Read** should be checked.
4. The optional device information just represents manufacturer details and model details. This information is used in two cases:
 - a. The device name is not specified – in this case a device name is automatically created from the optional device information. The name is concatenated to MAN_Medium_address, where MAN is the 3 character manufacturer code, Medium is the M-Bus medium (e.g. "Heat") and address is the specified address.
 - b. Device templates can be created from the M-Bus devices. The device templates store the device information in order to identify a device.

5. Click on the **Create Device** button. This creates the M-Bus device and adds it to the device list on the left hand side of the dialog.
6. When a device is selected the device information is displayed in the appropriate fields on the right hand side of the dialog. The information can be changed in the fields. Press the **Update Device** button to store the changes.
7. If a device has to be deleted select the device and press the **Remove Device** button.

To Add an M-Bus Device Manually Using the Scan Device Information

1. Enter the address of the device which has to be scanned.
2. Press the **Scan Device Information** button. If the device is found in the network, the device properties are filled.
3. Enter a name for the M-Bus device in the **Device Name** field. If no name is specified the name is created automatically as described in section 10.5.7.1 from the M-Bus data the device sends back.
4. Enter a device address in the **Device Address** field. If more devices with the same properties have to be created using subsequent addresses, the end address can be specified in the input field on the right hand side of the Device Address field.



5. Select a device Baud rate from the combo box.
6. Press the **Create Device** Button to add the number of devices.

To Add an M-Bus Device Manually Using a Template

1. Enter a name for the M-Bus device in the **Device Name** field. If no name is specified the name is created automatically as described in section 10.5.7.1 from the M-Bus data the device sends back.
2. Enter a device address in the **Device Address** field. If more devices with the same properties have to be created using subsequent addresses the end address can be specified in the input field on the right hand side of the **Device Address** field.



3. Click on the **Create From Template** button. This opens the **Import M-Bus Device Template** dialog shown in Figure 133.

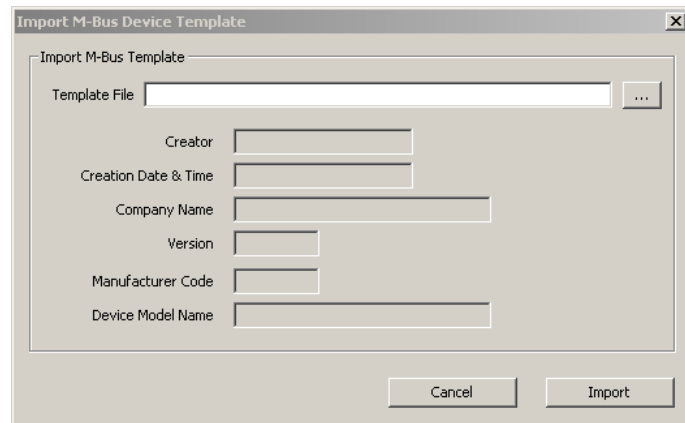


Figure 133 Import M-Bus Device dialog.

4. Press the button and select a template file from the **Open** dialog.
5. After selecting the file, the device information is displayed.
6. Press **Import** for importing the template or **Cancel** for closing the dialog without any changes.
7. When a template is imported, a folder with the name of the device is created. Under this folder a **Datapoints** folder containing the data points from the template file is created.

Tip: *Data points can be added to the data points of the template by right-clicking in the data point list and selecting **New Datapoint**.*

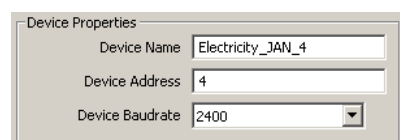
*When you want to create one or more device instance together with its data points, use the button **Create with DP** instead of the button **Create From Template**. This creates the device instance, all the data points from the template can be found in the **M-Bus Port's data points folder**.*

To Remove an M-Bus Device

1. Select the device which has to be removed, also multi-select is possible.
2. Press the **Remove Device** button. If the device already has data points, these data points have to be deleted before the remove can be performed.

To Change the Properties of an M-Bus Device

1. Select the device. This shows the device properties.



2. Update the field **Device Address** or select another Baud rate in the combo box.
3. Press the button **Update Device**.
4. If a device address is specified, which already exists, a failure message is displayed.

To Scan Devices Using the M-Bus Network Management Dialog

1. Scan for M-Bus devices as described in Section 10.5.7.2.
2. Start the scan by pressing the **Scan for Devices button**.
3. When the device scan is finished, the devices can be selected for a data scan. Also multi-select is possible.
4. Select the devices which have to be scanned for data points and press the **Scan Device Data** button. This scans all data points of the selected devices. For every device a folder with the name of the device is created under the **M-Bus Network Scan** folder. The data points found are placed in the **Datapoints** folder of the appropriate devices.

Important: *If a device, which is scanned, is already in the device list, the existing device can either be overwritten; deleting all previously scanned data points of the existing device or the scanned device can be discarded. A dialog is displayed for this decision.*

10.5.7.4 Manual Configuration of Data Points

It is possible to manually configure M-Bus data points. Manual configuration is done by specifying all information, the M-Bus device manufacturer provides.

To Manually Create an M-Bus Data Point

1. Click on the M-Bus port **Datapoints** folder.
2. Right click in the data point list view and select **New Datapoint** in the context menu.
3. This opens the **Create New M-Bus Datapoint** dialog shown in Figure 134.

Device Name	Device Address	Status	Data	Datapoints	Template
Other_REL_2	2	online	✖	0	
Heat_REL_1	1	online	✖	0	
Electricity_NZR_5_1	5	online	✔	6	
Water_INV_6	6	online	✖	0	
Electricity_JAN_4	4	online	✖	0	
Water_SEN_7	7	online	✖	0	

Datapoint Properties
 Datapoint Name:
 Object Type: Analog Input
☒ Enter Storage Number, Tariff, etc...
☐ Enter DIF/DIFE
 Storage Number:
 Tariff: [0 ... 255]
 Subunit: [0 ... 255]
 Function Field:
 Data Coding:
 DIF List: [FD:80:...]
 VIF List: [FD:80:...]
 Pollgroup:

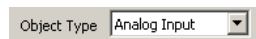
Figure 134 Create M-Bus Object dialog.

4. If the M-Bus device which provides the data point is not in the list, it has to be created. In this case open the Network Management dialog by clicking the Edit M-Bus Devices button.

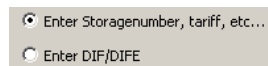
5. Create the device in the **Network Management** dialog and close the dialog.
6. Select the device which provides the M-Bus data point.
7. The data point properties are entered in the presented section of the dialog.
8. Enter a data point name. If no name is entered, the data point is named as described in section 10.5.7.1.

A screenshot of a text input field labeled 'Datapoint Name' with a small rectangular box next to it.

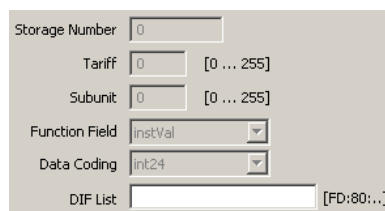
9. At the moment only analog M-Bus data points are supported. Select if the data point is an analog input or output. For analog inputs no M-Bus data coding can be specified.

A screenshot of a dropdown menu labeled 'Object Type' with 'Analog Input' selected.

10. Select if the data point shall be specified by providing the numbers for Storage number, tariff, subunit, function field and data coding or if the information configured using the DIF/DIFE list.

A screenshot of two radio buttons. The first is selected and labeled 'Enter Storagenumber, tariff, etc...'. The second is labeled 'Enter DIF/DIFE'.

For reference, if one piece of information is entered, the other one is derived from the specified data. Enter the data point information.

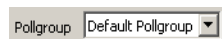
A screenshot of a configuration panel with several fields: 'Storage Number' (0), 'Tariff' (0) with range '[0 ... 255]', 'Subunit' (0) with range '[0 ... 255]', 'Function Field' (instVal), 'Data Coding' (int24), and 'DIF List' (empty) with range '[FD:80:...]'.

If the DIF list is entered, the dialog expects hexadecimal numbers. As soon as the information is entered the other fields are updated.

11. Enter the VIF/VIFE list. This list specifies the M-Bus counter type, and unit of the data point. Also this field has to be specified using hexadecimal numbers.

A screenshot of a text input field labeled 'VIF List' with a small rectangular box next to it.

12. Usually data points are added to a default poll group. If the data point has to be member of another poll group than default, the poll group can be selected using the drop down box.

A screenshot of a dropdown menu labeled 'Pollgroup' with 'Default Pollgroup' selected.

In the drop down box the previously specified poll groups are shown. If no poll group is configured only the default poll group is displayed. Refer to section 10.5.7.7 for more information on poll groups.

13. Press the **Create** button to create the M-Bus data point

Tip: *After creating a data point, the poll group can be changed in the data points property view. Also multi-select can be used.*

10.5.7.5 Importing via Device Templates

For some M-Bus devices special templates are available which specify all available data points of an M-Bus device as well as the device properties. Such templates can be imported into the configuration.

To import an M-Bus Device Template

1. Right click on the Folder **M-Bus Device Templates** and select **Import device template** from the context menu.
2. This opens the **Import M-Bus Device Template** dialog shown in Figure 135.

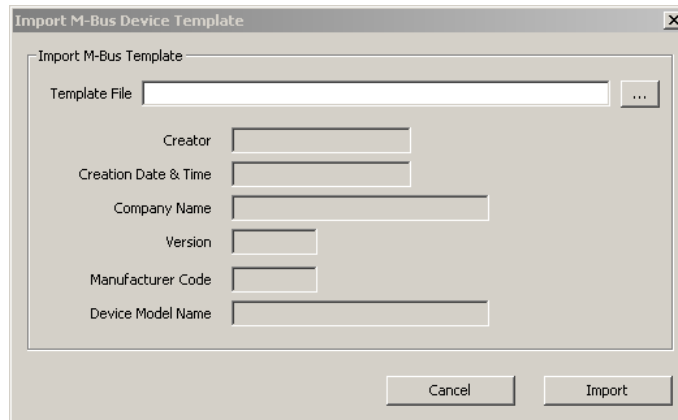


Figure 135 Import M-Bus Device Template dialog.

3. Press the  button and select a template file from the **Open** dialog.
4. After selecting the file, the device information is displayed.
5. Press **Import** for importing the template or **Cancel** for closing the dialog without any changes.
6. When a template is imported, a folder with the name of the device is created. Under this folder a **Datapoints** folder containing the data points from the template file is created.

Tip: *Data points can be added to the data points of the template by right clicking in the data point list and selecting **New Datapoint**.*

*Importing a device template from the folder list does not create a device instance. Device instances can only be created using the **import** in the **Network Management Dialog**.*

To Use Imported Data Points

Using imported data points is a little different to the use of scanned data points. For a scanned device a device instance already exists – the important information address and baud rate – devices imported from templates do not have an address or baud rate.

1. Go to the **Datapoints** folder of the device of the M-Bus Templates.
2. Select the desired data points, also multi-select is possible.

3. Either press on the **Use on Device** button  or right-click and select **Use on Device**. This opens the **M-Bus Configure Device For Use** dialog shown in Figure 136.

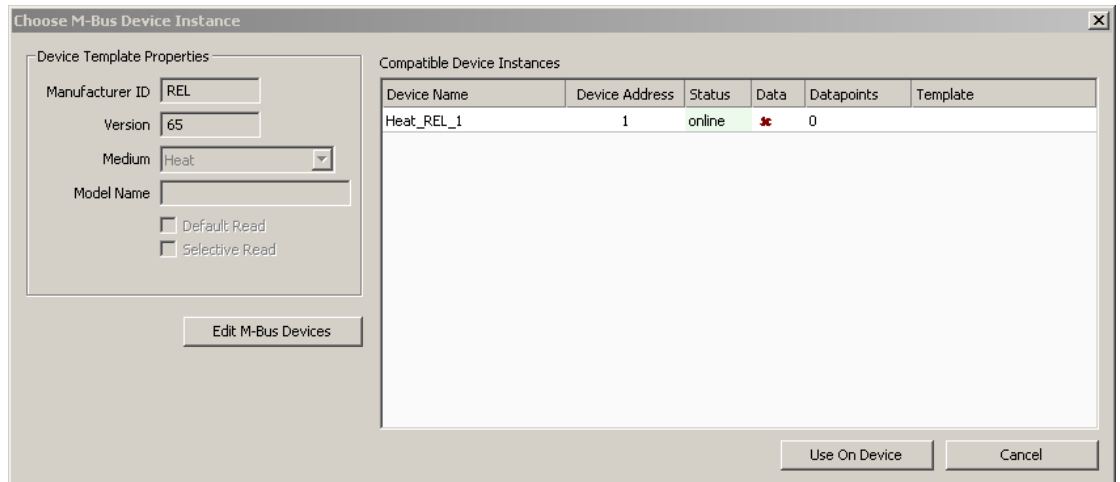


Figure 136 Use on Device dialog.

4. The device list displays all devices which have the same Manufacturer ID, version number and Medium. If no device instance matches the device template, create one by entering the network management dialog. The dialog can be entered by pressing the **Edit M-Bus Devices** button. In the management dialog, the device instance can be either created manually (take care of entering the correct Manufacturer ID, Version and Medium) or by simply importing the template again.
5. Select one or more device instances from the list and press the **Use On Device** button. This creates for each selected data point and each selected device one data point in the M-Bus Port's data point list.

10.5.7.6 Creating Device Templates

M-Bus device templates can be created from a data point configuration. In fact, it is only possible to create a device template using an existing device or an existing device template with data points. This device and its data points can either be configured manually, by a scan or also imported from a device template itself.

To Create an M-Bus Device Template Using Devices

1. Select the M-Bus dialog by clicking on the **M-Bus** button



in the tool bar of the **Datapoints** tab. This opens the **Network Management** dialog as displayed in Figure 137.

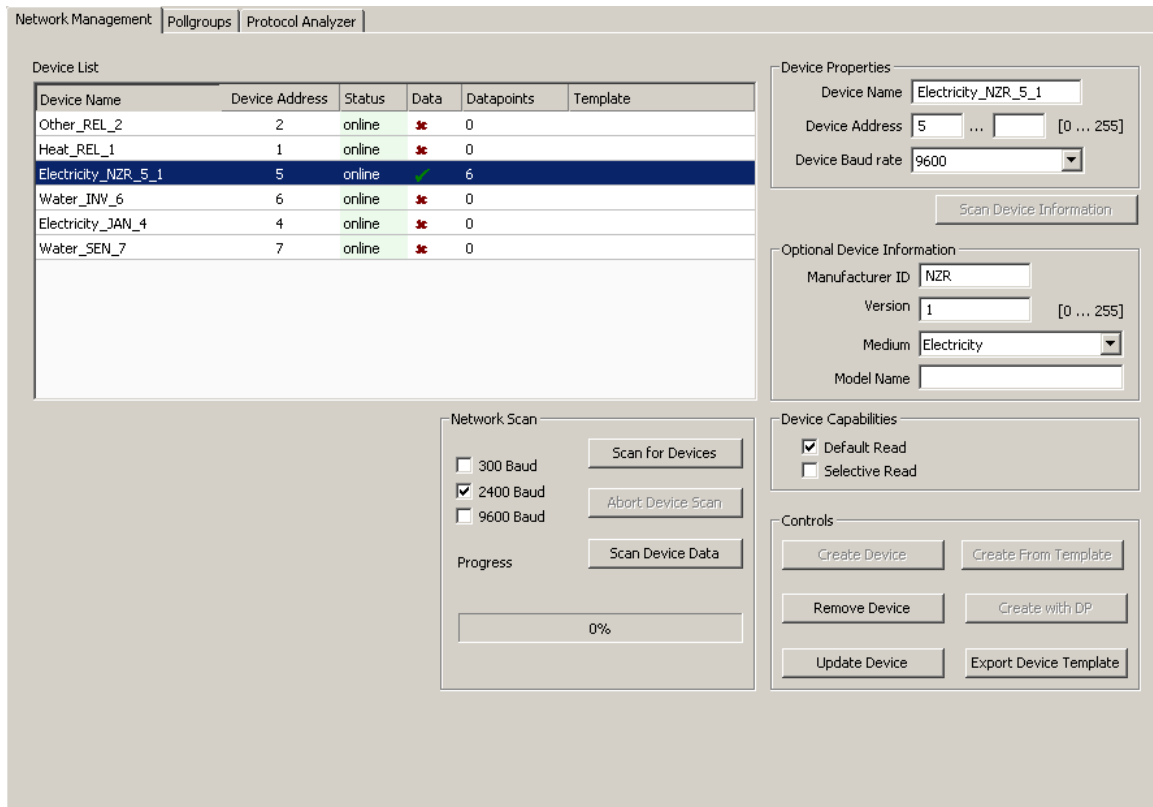
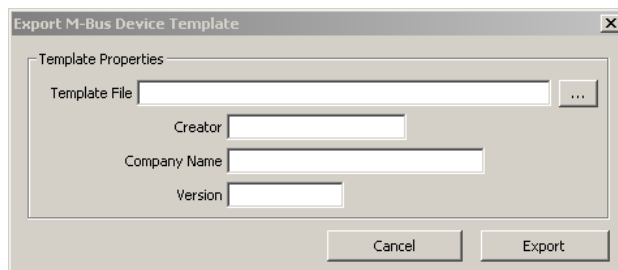


Figure 137 M-Bus Network Management dialog.

- The device list shows all devices of the current configuration. Select a device.
- Press the **Export Device Template** button. This opens the **M-Bus Export Template** dialog.



- Press the  button and select a template file from the **Save** dialog.
- Enter the **Creator**, **Company Name** and **Version** for the template. This information is stored in the template file, when importing the template file the information is displayed after selecting the file.
- Press the **Export** button.

To Create an M-Bus Device Template File Using a Device Template

- Right-click on the folder of the device template that has to be exported or its data point folder and select **Export Device Template...** from the context menu.
- Proceed as described above to export the template in the **Export M-Bus Device Template** dialog.

10.5.7.7 Pollgroups

In an M-Bus network, the master has to poll the slave devices. Input data points are therefore attached to a poll group. If nothing else is specified, the default poll group is used for input data points. The default poll group has a poll cycle of 60 seconds.

Three different types of poll groups can be specified:

- Time-based: The poll group is triggered on a time base. This means that after a specific time – the poll cycle – the poll group is processed.
- Trigger-based: The poll group is triggered on a special trigger data point. As soon as the trigger condition is met, the poll group is processed.
- Trigger-based with synchronization: This type is similar to the trigger-based. The difference is that when the trigger condition is met, a broadcast synchronization message is sent over the M-Bus. This causes the devices which are able to perform a sync operation to store special data points for later reading. After the broadcast is sent, the poll group is processed.

Tip: *If an M-Bus device is only able to process default read requests, it is advisable to attach all data points of this device to the same poll group (this increases the performance).*

The poll group a data point is attached to can be changed in the properties view of the data points. The poll group can also be changed for multiple data points using multi-select.

To Create a Time-Based M-Bus Poll Group

1. Select the **M-Bus** dialog by clicking on the **M-Bus** button



in the tool bar of the **Datapoints** tab. The **M-Bus Management** dialog opens.

2. Open the **Pollgroups** tab. This shows the dialog displayed in Figure 138.

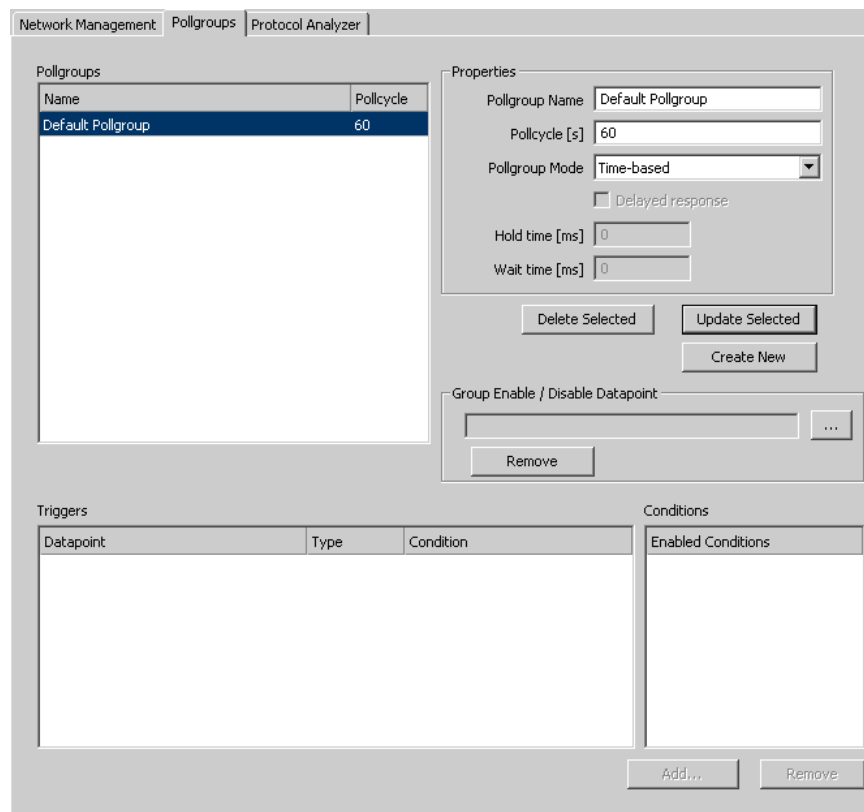


Figure 138: Pollgroup Management dialog.

3. The default poll group is selected and its properties are displayed. Enter the name of the new poll group and enter the poll cycle in seconds. Make sure that under **Pollgroup Mode** Time-based is selected.
4. Press the **Save** button to store the poll group and continue editing.
5. If a poll group needs to be updated or deleted, select the poll group edit the data and press the **Update Selected** or **Delete Selected** button.
6. Press the **Close** button to finish editing. When the poll groups have not been saved, a dialog asks whether the changes have to be saved or not.

To Create a Trigger-Based M-Bus Poll Group

1. Select the M-Bus dialog by clicking on the **M-Bus** button



in the tool bar of the **Datapoints** tab.

2. In the **M-Bus Management** dialog, open the **Pollgroups** tab. This displays the poll groups management tab displayed in Figure 138.
3. Enter a new poll group name and select **Trigger-based** or **Trigger-based with synchronization**.
4. Create the poll group by pressing the **Create New** button.
5. Select the new poll group. This enables the **Add...** and **Remove** buttons from the triggers.
6. Press the **Add...** button and select a trigger data point. This can for example be a binary user register.
7. The selected trigger data point appears in the trigger list as shown:

Triggers		
Datapoint	Type	Condition
Triggerdatapoint_Read	Value Update	-

8. Select the trigger from the list and check the desired trigger conditions.

Conditions	
Enabled Conditions	
☐	True (!= 0)
☐	False (== 0)
☐	Invalid
☐	Offline

9. The trigger conditions are then displayed in the trigger list.

Triggers		
Datapoint	Type	Condition
Triggerdatapoint_Read	Value Update	True (!= 0), False (== 0)

10. Press the **Close** button to leave the dialog.

10.5.7.8 Trending Synchronized Meter Data

The use of trigger-based poll groups with synchronization allows trending synchronized meter data. A trigger data point triggers a synchronization message over the M-Bus network. The M-Bus meters which are able to perform the synchronization action store the meter values. These values are read out afterwards.

To Trend Synchronized Meter Data

1. Create a binary trigger data point.

2. Create a trigger-based poll group with synchronization.
3. Create a trend log as described in Section 6.13. Set the Trend Mode to Change of Value (COV) and add all required data points.

10.5.7.9 M-Bus Protocol Analyzer

When connected to a device a protocol analyzer is available for the M-Bus port. The protocol analyzer can be found in the M-Bus Management dialog. Figure 139 shows the dialog for the M-bus protocol analyzer.

The status on the right hand side of the dialog shows, if the device is connected or if the protocol analyzer is stopped or started. When connected to a device, the protocol analyzer can be started by pressing the **Start Protocol** button. This starts the protocol analyzer in the device. Every time a transmission is made on the M-Bus port, the transmission is displayed in the list. Additionally the protocol data is stored in the device in a rotating log file. The protocol log can hold up to 40 kB of protocol data. So also when the Configurator was not running for an interesting time, the protocol data can be loaded from the device using the **Load From Device** button. The protocol data can be stored as CSV file using the **Save** button, with the **Clear** button, the shown protocol is deleted.

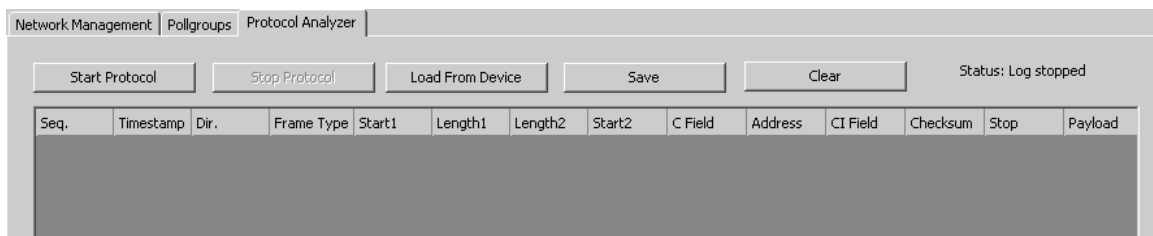


Figure 139 M-Bus protocol analyzer.

Figure 140 shows a typical protocol analyzer output for the M-Bus port. It shows the following information:

- **Seq.:** sequence number, which is automatically created in the device. This number is unique for one port.
- **Timestamp:** transmission time.
- **Frame Type:** M-Bus frame type (Short Frame, Control Frame Long Frame, E5 – in this case, no other data follows).
- **Dir.:** direction. Either SND (send) or RCV (receive)
- **Start1, Start2:** Start byte (must be equal)
- **Length1, Length2:** Frame length according to the M-Bus standard (must be equal)
- **C Field:** Control field
- **Address:** M-Bus address
- **CI Field:** Control information field
- **Checksum:** Checksum of the frame

- **Stop:** Stop byte
- **Payload:** Payload in hexadecimal numbers (this column cannot be used for sorting)

Some frame types do not contain the full set of fields. Please refer to the M-Bus standard for additional information.

Network Management | Pollgroups | Protocol Analyzer

Start Protocol

Stop Protocol

Load From Device

Save

Clear

Status: Log stopped

Seq.	Timestamp	Dir.	Frame Type	Start1	Length1	Length2	Start2	C Field	Address	CI Field	Checksum	Stop	Payload
68	2009-05-14 13:57:26.955	SND	Short Frame	10				5B	07		62	16	
69	2009-05-14 13:57:27.048	RCV	Long Frame	68	32	32	68	08	07	72	06	16	01 01 41 82 AE 4C 48 07 44 60 00 0C
70	2009-05-14 13:57:27.378	SND	Short Frame	10				7B	07		82	16	
71	2009-05-14 13:57:27.470	RCV	Long Frame	68	32	32	68	08	07	72	29	16	01 01 41 82 AE 4C 48 07 45 60 00 0C
72	2009-05-14 13:57:27.800	SND	Short Frame	10				5B	07		62	16	
73	2009-05-14 13:57:27.891	RCV	Long Frame	68	32	32	68	08	07	72	84	16	01 01 41 82 AE 4C 48 07 46 60 00 0C
74	2009-05-14 13:57:28.221	SND	Short Frame	10				7B	07		82	16	
75	2009-05-14 13:57:28.312	RCV	Long Frame	68	32	32	68	08	07	72	84	16	01 01 41 82 AE 4C 48 07 47 60 00 0C
76	2009-05-14 13:57:28.643	SND	Short Frame	10				5B	07		62	16	
77	2009-05-14 13:57:28.734	RCV	Long Frame	68	32	32	68	08	07	72	CA	16	01 01 41 82 AE 4C 48 07 48 60 00 0C
78	2009-05-14 13:57:29.064	SND	Short Frame	10				7B	07		82	16	

Figure 140 Typical protocol analyzer output for M-Bus port.

11 Modbus

11.1 Introduction

The Modbus is a de facto industrial standard which was initially intended for the communication between PLCs. In the meantime the Modbus has become an important interface for automatic meter reading applications and industrial applications. As the Modbus is an open protocol a large number of automation devices providing Modbus communication is available.

Two communication methods are available for Modbus. Modbus TCP utilizes Ethernet for the Modbus communication. Modbus RTU uses a RS485 bus for Modbus data transfer. Modbus RTU uses a serial bus, which is controlled by a single master. This master can request data from several slave devices connected to the network.

11.2 Modbus Network

Modbus TCP utilizes the Ethernet for the communication. Several Modbus slave devices can be connected. In Modbus TCP a unit identifier is used instead of the slave address. Modbus slaves may have the same unit identifier. This unifier is usually used to communicate with bridges, routers and gateways.

The Modbus RTU network utilizes an RS485 connection. Several Modbus slave devices are connected in parallel to the transmission medium. Each Modbus device has a unique slave address in the range from 1 to 255. The Baud rate of the RS485 can be configured to use 1200, 2400, 4800, 9600, 19200, and 38400 Baud. The parity is always none. The LOYTEC Modbus interface supports 8N1 only. Parity and stop bits are not configurable.

Modbus devices use function codes for the specification of the desired data. The following function codes for read/write actions are supported by the LOYTEC device:

- 02: Read discrete inputs.
- 01: Read coils.
- 05: Write coil.
- 04: Read input register
- 03: Read holding registers
- 06: Write holding registers

For optimizing the communication adjacent holding registers are usually read using a single read request. This behavior can be turned off for devices which do not support reading a random number of holding registers.

Modbus data points are specified by the function code, the address and the length. Furthermore, a data type has to be specified together with the information how the order of the bytes look like.

11.3 Web Interface

This section describes the Web interface for the Modbus port.

11.3.1 Port Configuration

The Modbus ports can be configured under the port configuration tabs of the Web UI (see Section 4.2.3). If available on a given port, the Modbus protocol can be enabled. If enabled, the Modbus communication settings on that port are displayed on the right-hand side. The RS485 port configuration tab is.

The screenshot displays the 'Port 1' configuration tab. On the left, there are radio buttons for 'Disable' and 'Modbus', with 'Modbus' being selected. Below these are 'Save Settings' and 'Get Settings' buttons. On the right, the configuration parameters are listed: 'Modbus port mode' is set to 'MASTER', 'Baud rate' is '38400 (default)', 'Parity' is 'NONE (default)', 'Mode' is 'RTU', 'Transmission Delay' is '0 (ms)', and 'Slave address' is '1 (1..255)'.

Figure 141 Modbus RS485 port configuration.

The settings for Modbus RS485 are displayed in Figure 141. For **Modbus port mode**, the following selections are available: **MASTER** can be selected, if the device shall operate as Modbus master. **SLAVE** can be selected, if the device shall operate as a Modbus slave on this port.

Under Baud rate the Baud rate for the Modbus communication can be configured. The available Baud rates are **1200, 2400, 4800, 9600, 19200, 38400 (default)**. Under Parity currently only **NONE** can be selected, using 1 stop bit. Parity and stop bits are not configurable. The **Mode** specifies if the communication shall use the Modbus **RTU** mode or the Modbus **ASCII** mode.

If operated as Modbus master, an additional **Transmission delay** can be defined in milliseconds. This can improve communications on Modbus RS485 with slow devices that operate outside the timing specifications. Normally, leave this setting at '0'. As a Modbus slave, the user needs to define a unique **slave address** that this port will have on the Modbus channel.

Press the button **Save Settings** for storing the parameter configuration into the device or press **Get Settings** for overwriting the changes with the original configuration.

Figure 142 Modbus TCP port configuration.

On an Ethernet port, Modbus TCP can be enabled by selecting the check box. The Modbus TCP communication settings are displayed on the right-hand side as shown in Figure 142. For **Modbus port mode**, the following selections are available: **MASTER** can be selected, if the device shall operate as Modbus master. **SLAVE** can be selected, if the device shall operate as a Modbus slave on this port. Configure the desired TCP port, which is used by Modbus TCP devices on that channel. The default Modbus port number is 502.

11.3.2 Data Points

Modbus data points can be accessed through the Web UI as described in Section 4.2.11.

11.3.3 Statistics

Figure 143 shows a typical output of the statistics information which can be displayed for the Modbus ports. For each port available one statistics tab is displayed. The statistics can be cleared for each Modbus port separately by pressing the **Clear Modbus statistics** button. A refresh of the statistics can be done by pressing **Update Modbus statistics**.

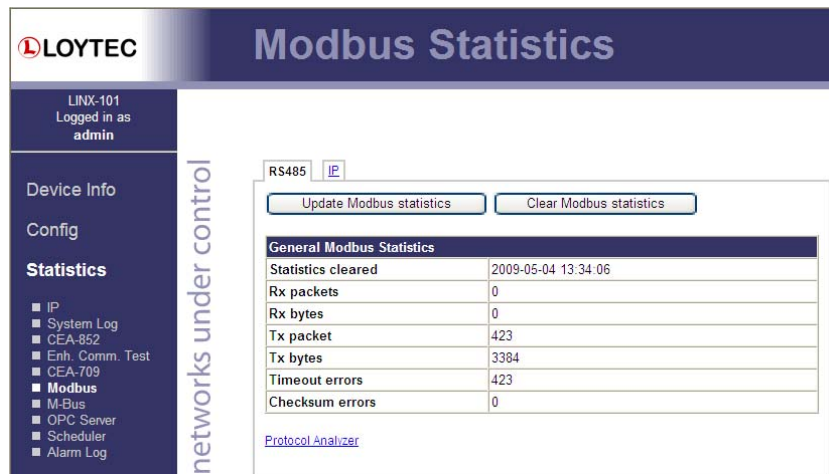


Figure 143: Statistics of the Modbus port.

The following information is available:

- Statistics cleared: last time of statistics reset
- Rx packets: number of Modbus packets received
- Rx bytes: number of bytes received
- Tx packets: number of Modbus packets sent
- Tx bytes: number of bytes sent
- Timeout errors: number of communication errors (timeout)

- Checksum errors: number of communication errors (wrong checksum)

11.3.4 Modbus Protocol Analyzer

By activating the link Protocol Analyzer (available in all Modbus statistics tabs), the protocol analyzer page is shown as displayed in Figure 144.

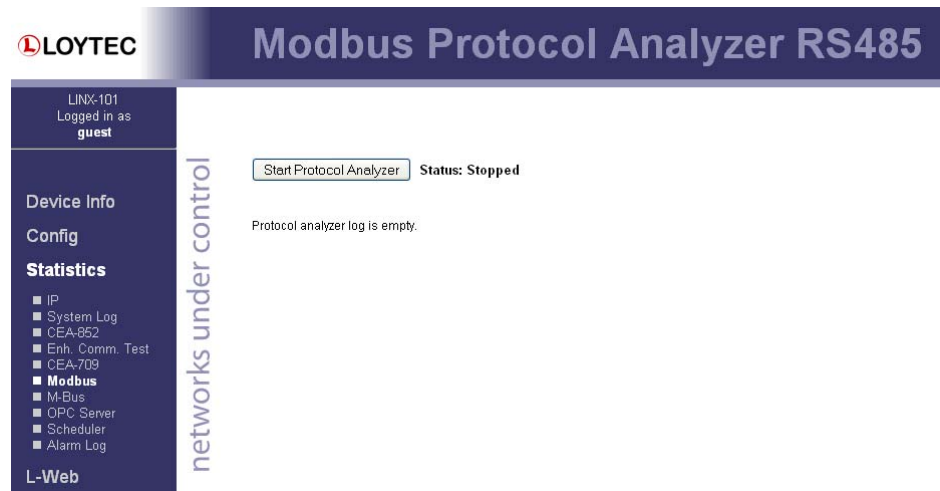


Figure 144 Modbus protocol analyzer.

Next to the button the status of the protocol analyzer is shown. If the analyzer is started, an automatic refresh is performed every 60 seconds. By pressing the button **Start Protocol Analyzer** / **Stop Protocol Analyzer** the protocol analyzer can be started / stopped.

For every frame sent or received a line is presented using comma separated values.

11.4 Configurator

This section describes how to use the Configurator software for the management of Modbus data points. For further information on the Configurator software refer to Chapter 6.

11.4.1 Activating Modbus Configuration

Before a new Modbus configuration can be managed, the Modbus option must be enabled for the appropriate port. The project settings are described in detail in Section 6.3.

To Activate the Modbus Configuration

1. Open the project settings dialog.

2. In the **Device Config** tab enable the Modbus check boxes on the desired ports as shown in Figure 145. Setting the check box enables Modbus on that port. Edit the Modbus communication settings.
3. If slave mode is enabled, you may change the default Modbus register layout in the **Modbus Slave Register Configuration** box.
4. Click the **Download** button to activate the changes in the configuration.

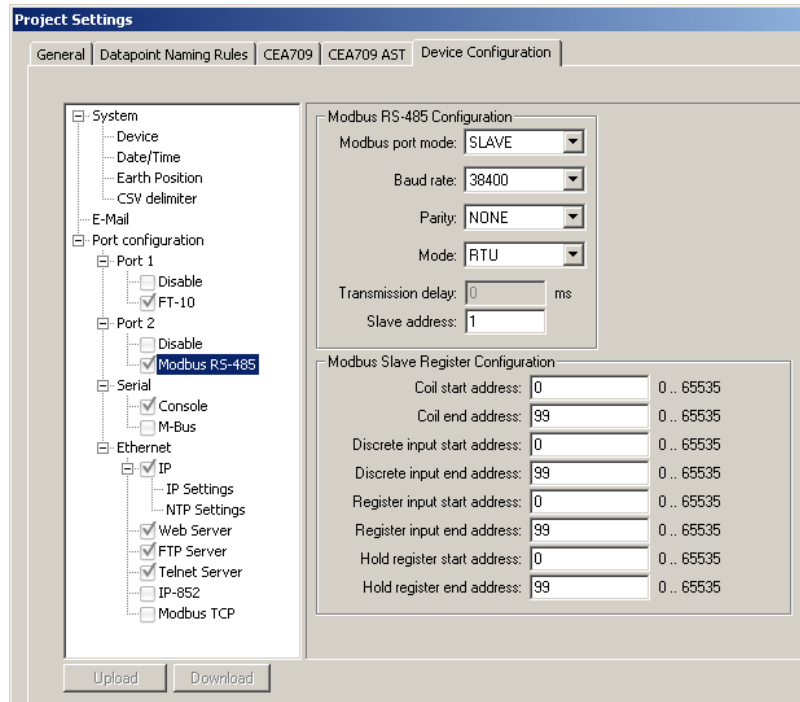


Figure 145: Project settings for Modbus.

Important: *If the Modbus port is deactivated via the check box or a firmware or model version is chosen, which does not support Modbus, the entire Modbus configuration is deleted. In this case a dialog is displayed, which has to be confirmed.*

11.4.2 Data Point Manager for Modbus

The Configurator uses a central concept to manage data points. The data point manager as shown in Figure 146 is used to select, create, edit and delete data points. The dialog is divided into three sections:

- The folder list (Figure 146),
- The data point list (Figure 147),
- And a property view.

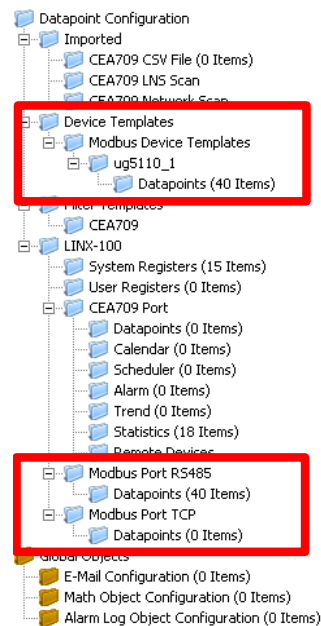


Figure 146 : Data Point Manager Dialog with Modbus folder list.

No.	OPC	Direction		Datapoint Name	Device Name	Start Address	Register Type	Data Length	ID
1	☒	In		VARh_cap_net	ug5110_1_1	180	HOLD	4	1065
2	☒	In		VARh_ind_net	ug5110_1_1	178	HOLD	4	1066
3	☒	In		VAh_net	ug5110_1_1	176	HOLD	4	1067
4	☒	In		Wh_net	ug5110_1_1	174	HOLD	4	1068
5	☒	In		VARh_cap_del	ug5110_1_1	172	HOLD	4	1069
6	☒	In		VARh_ind_del	ug5110_1_1	170	HOLD	4	106A
7	☒	In		VAh_del	ug5110_1_1	168	HOLD	4	106B

Figure 147: Datapoint Manager Dialog with Modbus Data Point List.

11.4.3 Folder List

At the left is a list of folders which is used to sort the available data objects by their category. There are a number of predefined Modbus folders available. All other folders are described in Section 6.2.1:

- **Device Templates:** This folder contains created data point templates for the different technologies.
 - **Modbus Device Templates:** This folder contains a sub-folder for each device, which is imported from an Modbus device template. This device folder also contains a sub-folder with the data points specified in the template. Data points can be added to the folder. Additionally suitable data objects can be created for the use on the device by selecting the **Use on Device** option.
- **LINX-10X:** This is the device folder of the LINX-10X. It contains all the necessary data points which constitute to the LINX-10X's port interface definition. These data points are created on the LINX-10X when the configuration is downloaded. For Modbus additional sub-folders exist:
 - **Modbus Port RS-485:** This folder contains the remote Modbus data points of the Modbus RS-485 port, which are used on the device.
 - **Modbus Port TCP:** This folder contains the remote Modbus data points of the Modbus TCP port, which are used on the device.

Using the context menu on a folder, sub-folders may be created to organize the available objects. If new objects are created automatically, they are usually placed in the base folder

and can then be moved by the user to any of his sub-folders. Note, that the folder structure described above cannot be changed by adding or deleting folders at that level.

11.4.4 Network Port Folders

The Modbus network port folder on the device has the same structure of sub-folders as the other network port folders in Section 6.2.2. Currently only the **Datapoints** folder exists for the Modbus network ports.

11.4.5 Modbus Properties

Apart from the common data point properties discussed in Section 6.2.4 the data points of the Modbus technology have additional properties:

- **Modbus Device Name:** This property defines the name of the Modbus slave device which contains the data point.
- **Modbus Device Address:** This property defines the address of the Modbus slave device which contains the Modbus data point.
- **Modbus Register Start Address:** This property defines the address of the Modbus register.
- **Modbus Register Type:** This property defines the register type of the data point. Also the function code, which specifies the register, is displayed. When the Modbus register type is changed from a read to a write register, also the direction of the data point is changed.
- **Modbus Data Type:** This property defines the representation of data in the slave. This is the data type the Modbus slave uses for the data point internally. This can for example be float, double, int16 or uint32.
- **Modbus Multiplier, Exponent and Offset:** This property defines scaling parameters for the data point. The value of the data point in the LOYTEC device is calculated as follows:

$$\text{Value} = (\text{ModbusValue} + \text{Offset}) \cdot \text{Multiplier} \cdot 10^{\text{Exponent}}$$

- **Modbus Swap 16 bit, Swap 32 bit and Swap 64 bit:** This information specifies, if the order of received Modbus data has to be changed. When Swap 16 bit is set, the two bytes of a 16 bit word are swapped, if Swap 32 is set, the two words of 32 bit are swapped, and if Swap 64 bit is set, the two 32 bit words of 64 bit long data are swapped. Also combinations are possible. This configuration is necessary because the Modbus slaves can store information in any byte order (the Modbus protocol only specifies, how 16 bit data is transferred).
- **Pollgroup:** This property is only available for input data points. It shows the poll group, the data point is connected to.

11.4.6 Modbus Workflow

This section discusses the workflows for setting up a Modbus environment. Modbus does not provide a scan function and therefore the network has to be setup offline. This can be eased by the use of templates. If no templates are available, the data points have to be set up manually.

Figure 148 describes the workflow for setting up a Modbus network. For using Modbus the Modbus ports of the LOYTEC device and the Modbus devices have to be configured. The RS-485 Modbus port must get a Baud rate, the parity is fixed at none and the stop bits are configured to 2. The Modbus TCP port must get the TCP port number of the slave devices. The Modbus devices have to be configured according to the LOYTEC device's port configuration. When no device template is available for a Modbus device, it can simply be created by configuring the Modbus data points for the device and exporting the device template. The exported device template can then be used to easily add additional Modbus

devices with the same data point configuration. Also mixing the two methods is possible. When using the device templates also data points can be added manually. The configuration is then downloaded to the device and the device is rebooted.

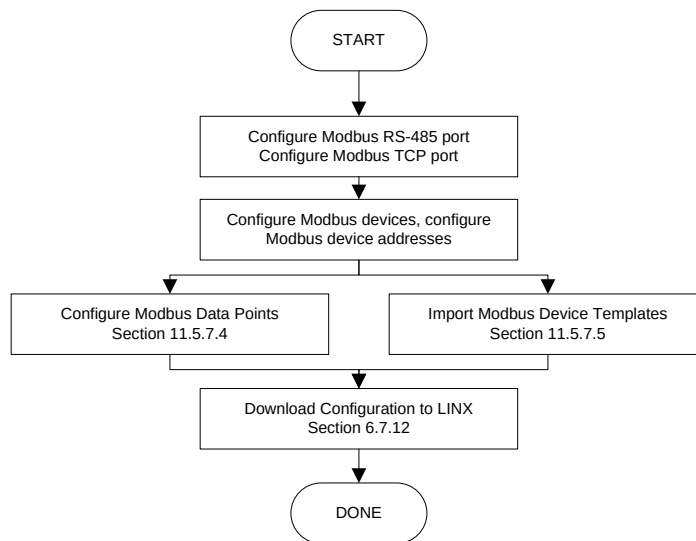


Figure 148: Workflow for offline engineering.

11.4.7 Using the Configurator for Modbus

11.4.7.1 Modbus Management Functions

This section describes how the Modbus network management functions can be used. It describes adding and removing Modbus.

The **Modbus Management** dialog shown in Figure 149 shows the list of devices. Devices which have been imported from a template show the template name in the last column. For each device the address, the IP address (if available), the port and the number of data points available on that device is shown.

The Modbus Management dialog can also be used for the configuration of poll groups and for accessing the LOYTEC devices protocol analyzer.

To Start the Modbus Network Management Dialog

1. Connect to the device via FTP as described in section 6.7.2.
2. Select the Modbus dialog by clicking on the **Modbus** button



in the tool bar of the **Datapoints** tab. The Modbus Management dialog opens, showing the **Modbus Device Management** tab displayed in Figure 149.

Modbus Device Management | Pollgroups | Protocol Analyzer RS-485 | Protocol Analyzer TCP

Device Name	Device Address	IP Address	Port	Datapoints	Template
ug5110_1_1_44	44		RS-485	45	elmeasuretempla...
moddev_1	1		RS-485	0	
moddev_2	2		RS-485	0	
moddev_3	3		RS-485	0	
ug5110_1_1_0_1	1	192.168.34.0	TCP	45	elmeasuretempla...

Device Properties

Type: RS-485

Device Name:

Device Address: [1 .. 255]

Device IP Address: . . .

Number of Devices:

☒ Increase Device Address

☐ Read Single Registers

Manufacturer Details

Manufacturer:

Model:

Device Operations

Create Device Create From Template

Remove Device Create with DP

Update Device Export Device Templ.

Figure 149: Modbus management dialog.

To Add a Modbus Device Manually

1. Fill in the **Device Address** and select the **Type** (either RS485 or TCP) from the drop down box.
2. A **Device Name** can be specified. If no device name is specified, the device name is created automatically. If more devices with the same properties have to be created using subsequent addresses, the number of devices can be specified in the input field under the **Device IP Address** field. If a number of TCP devices has to be created, subsequent IP addresses are configured. If the checkbox **Increase Device Address** is checked, also the Device Addresses (unit IDs) of the TCP devices are increased.

Number of Devices

3. The **Device Address** specifies the address of the Modbus device ranging from 1 to 255. In case of a TCP device the device address specifies the unit ID. For a RS-485 device the device address has to be unique, TCP devices can have equal device addresses.
4. For TCP devices the **Device IP Address** has to be specified.
5. If the device is not able to read adjacent registers with one read command, activate the checkbox **Read Single Registers**.
6. The optional manufacturer details just represent **Manufacturer** name and **Model** name. This information is used to identify device templates.
7. Click on the **Create Device** button. This creates the Modbus device and adds it to the device list on the left hand side of the dialog.
8. When a device is selected the device information is displayed in the appropriate fields on the right hand side of the dialog. The information can be changed in the fields. Press the **Update Device** button to store the changes.
9. If a device has to be deleted select the device and press the **Remove Device** button.

To Add a Modbus Device Manually Using a Template without Creating Data Points

1. Enter a name for the Modbus device in the **Device Name** field. If no name is specified the name is created automatically from the name in the template file.
2. Fill in the **Device Address** and select the **Type** (either RS485 or TCP) from the drop down box. If TCP is selected also enter the **Device IP Address**. If more devices with the same properties have to be created using subsequent addresses, the number of devices can be specified in the input field under the **Device IP Address** field.

Number of Devices

3. Click on the **Create From Template** button. This opens the **Import Modbus Device Template** dialog shown in Figure 150.

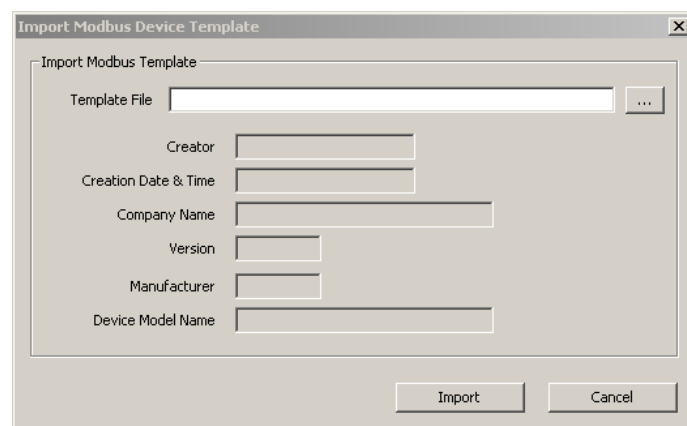


Figure 150 Import Modbus Device Template dialog.

4. Press the button and select a template file from the **Open** dialog.
5. After selecting the file, the device information is displayed.
6. Press **Import** for importing the template or **Cancel** for closing the dialog without any changes.
7. When a template is imported, a folder with the name of the device is created. Under this folder a **Datapoints** folder containing the data points from the template file is created.

Tip: *Data points can be added to the data points of the template by right-clicking in the data point list and selecting New Datapoint.*

To Add a Modbus Device Manually Using a Template Creating Data Points

1. Enter a name for the Modbus device in the **Device Name** field. If no name is specified the name is created automatically from the name in the template file.
2. Fill in the **Device Address** and select the **Type** (either RS485 or TCP) from the drop down box. If TCP is selected also enter the **Device IP Address**. If more devices with the same properties have to be created using subsequent addresses, the number of devices can be specified in the input field under the **Device IP Address** field.

Number of Devices

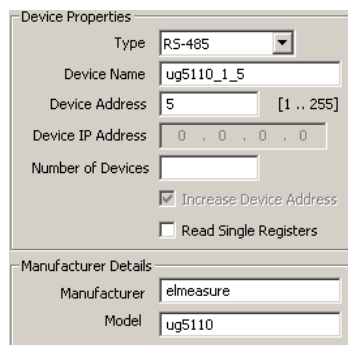
3. Click on the **Create with DP** button. This opens the **Import Modbus Device Template** dialog shown in Figure 150.
4. Press the  button and select a template file from the **Open** dialog.
5. After selecting the file, the device information is displayed.
6. Press **Import** for importing the template or **Cancel** for closing the dialog without any changes.
7. When a template is imported, a folder with the name of the device is created. Under this folder a **Datapoints** folder containing the data points from the template file is created.
8. The created device is shown in the list together with the number of data points.

To Remove a Modbus Device

1. Select the device which has to be removed, also multi-select is possible.
2. Press the **Remove Device** button. If the device already has data points, these data points have to be deleted before the remove can be performed.

To Change the Properties of a Modbus Device

1. Select the device. This shows the device properties.



The image shows a 'Device Properties' dialog box. It has two main sections. The top section contains fields for 'Type' (a dropdown menu showing 'RS-485'), 'Device Name' (a text box with 'ug5110_1_5'), 'Device Address' (a text box with '5' and a range '[1 .. 255]'), 'Device IP Address' (a text box with '0 . 0 . 0 . 0'), and 'Number of Devices' (a text box). Below these are two checkboxes: 'Increase Device Address' (checked) and 'Read Single Registers' (unchecked). The bottom section is titled 'Manufacturer Details' and contains 'Manufacturer' (a text box with 'elmeasure') and 'Model' (a text box with 'ug5110').

2. Update the properties which have to be changed.
3. Press the button **Update Device**.
4. When the device type is changed, it is verified that no device with the address exists on the appropriate port – on RS485 the device address has to be unique, on TCP the device IP address has to be unique.

11.4.7.2 Manual Configuration of Data Points

It is possible to manually configure Modbus data points. Manual configuration is done by specifying all information, the Modbus device manufacturer provides.

To Manually Create an Modbus Data Point

1. Click on the Modbus port **Datapoints** folder.
2. Right-click in the data point list view and select **New Datapoint...**

- This opens the **Create New Modbus Datapoint** dialog showing only the devices which are available on the appropriate port. This dialog is shown in Figure 151.

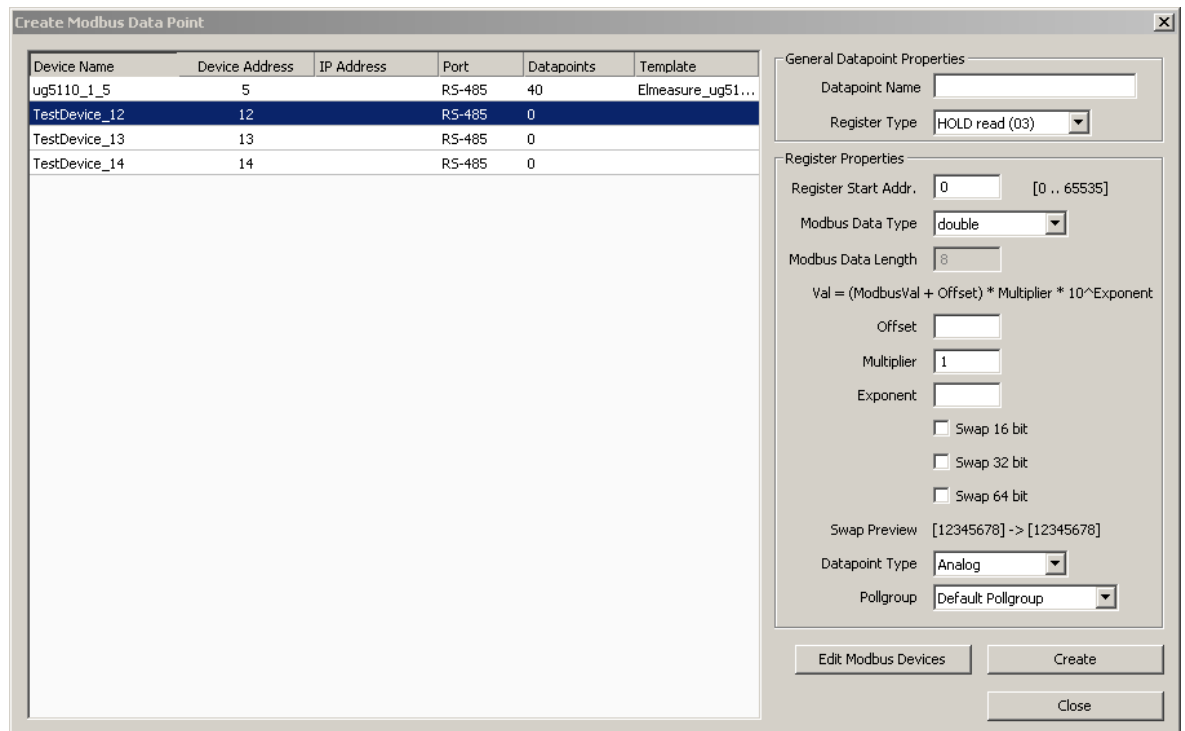
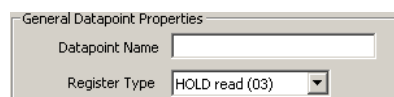


Figure 151 Create Modbus Datapoint dialog.

- If the Modbus device which provides the data point is not in the list, it has to be created. In this case open the Modbus Management dialog by clicking the Edit Modbus Devices button.
- Create the device in the **Modbus Management** dialog and close the dialog.
- Select the device which provides the Modbus data point.
- Enter the General Data Point Properties. These are the **data point name**, which is automatically created when not specified, and the **Register Type**. The register type of the data point is provided in the Modbus device documentation. The drop down menu shows the Modbus register type, the direction (read and write) and the function code. The data point properties are entered in the presented section of the dialog.

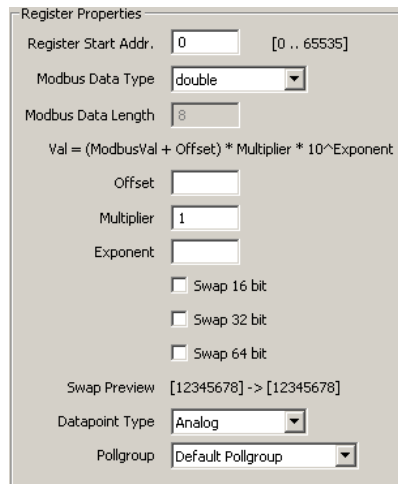


- Enter the properties of the data point. The register address is specified by the manufacturer. Select the **Modbus Data Type**. This type specifies how the manufacturer stores data in the Modbus device. The **Modbus Data Length** is automatically updated according to the data type. Offset, Multiplier and Exponent can be used for mapping purposes. The Value of the data point is calculated as follows:

$$\text{Value} = (\text{ModbusValue} + \text{Offset}) \cdot \text{Multiplier} \cdot 10^{\text{Exponent}}$$

Modbus does not specify any byte orders of the data stored in devices. For some devices it may be necessary to change the byte order. This is done by the check boxes **Swap 16 bit**, **Swap 32 bit** and **Swap 64 bit**. When Swap 16 bit is activated, the 2 byte

of a word are swapped, when Swap 32 bit is activated, the 2 words of a 32 bit value are swapped and if Swap 64 bit is activated, the two 32 bit words of a 64 bit value are swapped. A preview of the byte order is shown under the check boxes. Select the **Data Point Type** of the data point (analog value, multi-state or binary) – only the types which are available for the register type-data type combination are shown.



The image shows a 'Register Properties' dialog box with the following fields and options:

- Register Start Addr: 0 [0 .. 65535]
- Modbus Data Type: double
- Modbus Data Length: 8
- Val = (ModbusVal + Offset) * Multiplier * 10^Exponent
- Offset: [empty]
- Multiplier: 1
- Exponent: [empty]
- Swap 16 bit: ☐
- Swap 32 bit: ☐
- Swap 64 bit: ☐
- Swap Preview: [12345678] -> [12345678]
- Datapoint Type: Analog
- Pollgroup: Default Pollgroup

9. Select a poll group for read data points from the **Pollgroup** drop down box. The drop down box is grayed out for write registers. Additional poll groups can be configured in the Modbus Management dialog.
10. Press the **Create** button to create the Modbus data point.
11. After the point is created the dialog is not closed, so additional data points can be created.

Tip: *After creating a data point, the poll group can be changed in the data points property view. Also multi-select can be used in the data point property view.*

11.4.7.3 Importing via Device Templates

For some Modbus devices special templates are available which specify all available data points of a Modbus device as well as the device properties. Such templates can be imported into the configuration.

To import a Modbus Device Template

1. Right click on the Folder **Modbus Device Templates** and select **Import device template** from the context menu.
2. This opens the **Import Modbus Device Template** dialog shown in Figure 152.

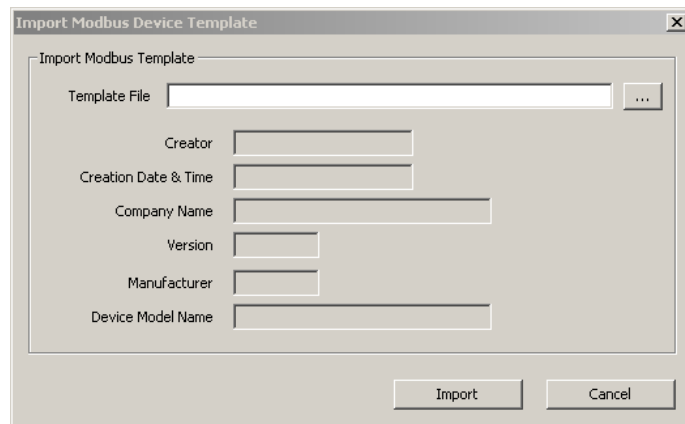


Figure 152 Import Device Template dialog.

3. Press the  button and select a template file from the **Open** dialog.
4. After selecting the file, the device information is displayed.
5. Press **Import** for importing the template or **Cancel** for closing the dialog without any changes.
6. When a template is imported, a folder with the name of the device is created. Under this folder a **Datapoints** folder containing the data points from the template file is created.

Tip:	<i>Data points can be added to the data points of the template by right clicking in the data point list and selecting New Datapoint.</i>
	<i>Importing a device template from the folder list does not create a device instance. Device instances can only be created using the import in the Network Management Dialog. In this dialog also the device instances can also be created with their data points.</i>

To Use Imported Data Points using Use On Device

1. Go to the **Datapoints** folder of the device of the Modbus Templates.
2. Select the desired data points, also multi-select is possible.

3. Either press on the **Use on Device** button  or right-click and select **Use on Device**. This opens the **Choose Modbus Device Instance** dialog.

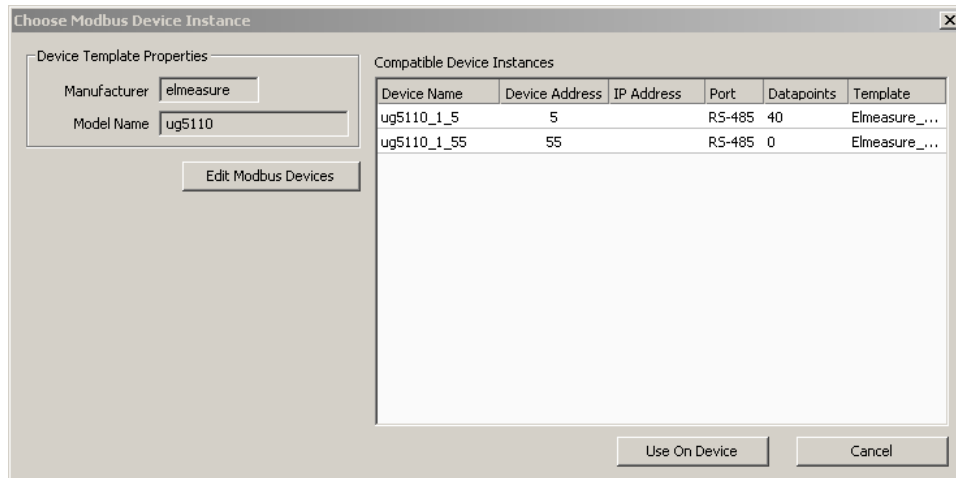


Figure 153: Choose Modbus Device Instance dialog.

4. The device list displays all devices which have the same Manufacturer, and the same Model Name as the template. If no device instance matches the device template, create one by entering the Modbus management dialog. The dialog can be entered by pressing the **Edit Modbus Devices** button. In the management dialog, the device instance can be either created manually (take care of entering the correct manufacturer and model) or by simply importing the template again.
5. Select one or more device instances from the list and press the **Use On Device** button. This creates for each selected data point and each selected device one data point in the Modbus Port's data point list.

11.4.7.4 Creating Device Templates

Modbus device templates can be created from a data point configuration. In fact, it is only possible to create a device template using an existing device or an existing device template with data points. This device and its data points can either be configured manually or also imported from a device template itself.

To Create a Modbus Device Template Using Devices

1. Select the Modbus dialog by clicking on the **Modbus** button



in the tool bar of the **Datapoints** tab. This opens the **Network Management** dialog opens as described in Section 11.4.7.1.

2. The device list shows all devices of the current configuration. Select the device you want to export.

Device Name	Device Address	IP Address	Port	Datapoints	Template
ug5110_1_5_5	5		R5-485	3	
TestDevice_14_14	14		R5-485	0	

- Press the **Export Device Templ.** button. This opens the **Export Modbus Device Template** dialog shown in Figure 154. The list on the left side of the dialog shows the names of the data points which are exported to the template.

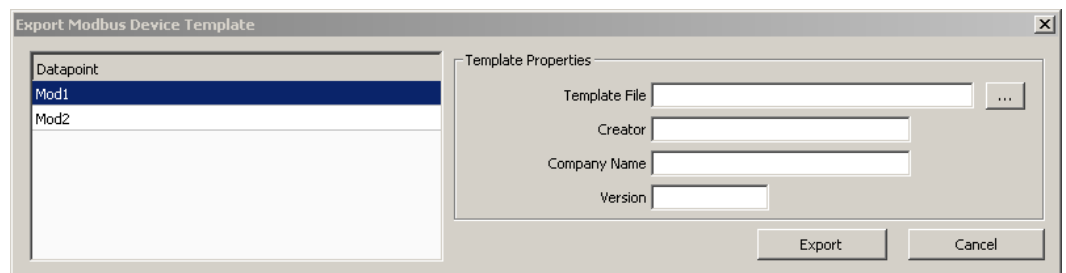


Figure 154 Export Modbus Device Template dialog.

- Press the  button and select a template file from the **Save** dialog.
- Enter the **Creator**, **Company Name** and **Version** for the template. This information is stored in the template file, when importing the template file the information is displayed after selecting the file.
- Press the **Export** button.

To Create a Modbus Device Template File Using a Device Template

- Right-click on the folder of the device template that has to be exported or its data point folder and select **Export Device Template...** from the context menu.
- This opens the **Export Modbus Device Template** dialog as shown in Figure 154. Proceed as described above.

11.4.7.5 Pollgroups

In a Modbus network, the master has to poll the slave devices. Input data points are therefore attached to a poll group. If nothing else is specified, the default poll group is used for input data points. The default poll group has a poll cycle of 60 seconds.

Two different types of poll groups can be specified:

- Time-based: The poll group is triggered on a time base. This means that after a specific time – the poll cycle – the poll group is processed.
- Trigger-based: The poll group is triggered on a special trigger data point. As soon as the trigger condition is met, the poll group is processed.

Tip: *The poll group a data point is attached to can be changed in the properties view of the data points. The poll group can also be changed for multiple data points using multi-select.*

To Create a Time-Based Poll Group

- Select the Modbus dialog by clicking on the **Modbus** button



in the tool bar of the **Datapoints** tab. This opens the **Modbus Management** dialog.

2. Open the **Pollgroups** tab. This shows the dialog displayed in Figure 155.

Name	Pollcycle
Default Pollgroup	60

Properties

Pollgroup Name: Default Pollgroup

Pollcycle [s]: 60

Pollgroup Mode: Time-based

☐ Delayed response

Hold time [ms]: 0

Wait time [ms]: 0

Delete Selected Update Selected Create New

Group Enable / Disable Datapoint: [] ...

Remove

Triggers

Datapoint	Type	Condition
-----------	------	-----------

Conditions

Enabled Conditions

Add... Remove

Figure 155: Pollgroup Management dialog.

3. The default poll group is selected and its properties are displayed. Enter the name of the new poll group and enter the poll cycle in seconds. Make sure that under **Pollgroup Mode** Time-based is selected.
4. Press the **Save** button to store the poll group and continue editing.
5. If a poll group needs to be updated or deleted, select the poll group, edit the data and press the **Update Selected** or **Delete Selected** button.
6. Press the **Close** button to finish editing. When the poll groups have not been saved, a dialog asks whether the changes have to be saved or not.

To Create a Trigger-Based Modbus Poll Group

1. Select the Modbus dialog by clicking on the **Modbus** button



in the tool bar of the **Datapoints** tab. This opens the **Modbus Management** dialog.

2. In the **Modbus Management** dialog, open the **Pollgroups** tab. This displays the poll groups management tab displayed in Figure 155.
3. Enter a new poll group name and select **Trigger-based**.
4. Create the poll group by pressing the **Create New** button.
5. Select the new poll group. This enables the **Add...** and **Remove** buttons from the triggers.
6. Press the **Add...** button and select a trigger data point. This can for example be a binary user register.
7. The selected trigger data point appears in the trigger list as shown:

Triggers		
Datapoint	Type	Condition
Triggerdatapoint_Read	Value Update	-

8. Select the trigger from the list and check the desired trigger conditions.

Conditions	
Enabled Conditions	
☐	True (!= 0)
☐	False (== 0)
☐	Invalid
☐	Offline

9. The trigger conditions are then displayed in the trigger list.

Triggers		
Datapoint	Type	Condition
Triggerdatapoint_Read	Value Update	True (!= 0), False (== 0)

10. Press the **Save** button to store the changes in the poll groups.

11.4.7.6 Modbus Protocol Analyzer

When connected to a device a protocol analyzer is available for each Modbus port. The protocol analyzer can be found in the Modbus Management dialog. On every Modbus port a protocol analyzer tab is available. Figure 156 shows the Modbus protocol analyzer

The status on the right hand side of the dialog shows, if the device is connected or if the protocol analyzer is stopped or started. When connected to a device, the protocol analyzer can be started by pressing the **Start Protocol** button. This starts the protocol analyzer in the device. Every time a transmission is made on the Modbus port, the transmission is displayed in the list. Additionally the protocol data is stored in the device in a rotating log file. The protocol log can hold up to 40 kB of protocol data. So also when the Configurator

was not running for an interesting time, the protocol data can be loaded from the device using the **Load From Device** button. The protocol data can be stored as CSV file using the **Save** button, with the **Clear** button, the shown protocol is deleted.

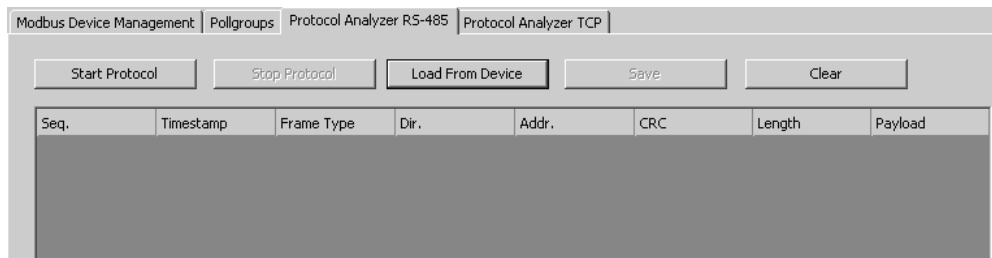


Figure 156 Modbus protocol analyzer.

Figure 157 shows a typical protocol analyzer output for the Modbus TCP port. It shows the following information for TCP:

- **Seq.:** sequence number, which is automatically created in the device. This number is unique for one port.
- **Timestamp:** transmission time.
- **Frame Type:** 'TCP' or 'Damaged' when something happened with the frame.
- **Dir.:** direction. Either SND (send) or RCV (receive)
- **Trans ID:** Transaction ID
- **Prot ID:** Protocol ID
- **Unit ID:** Unit ID
- **Length:** Payload length of the data frame
- **Payload:** Payload in hexadecimal numbers (this column cannot be used for sorting).

Seq.	Timestamp	Frame Type	Dir.	Trans ID	Prot ID	Unit ID	Length	Payload
7312	2009-05-06 17:48:14.094	TCP	SND	8740	0	1	12	22 24 00 00 00 06 01 03 00 00 00 0C
7313	2009-05-06 17:48:14.116	TCP	RCV	8740	0	1	33	22 24 00 00 00 1B 01 03 18 40 D2 17 80 00 00 00 00 40 D2
7314	2009-05-06 17:48:14.120	TCP	SND	8741	0	1	12	22 25 00 00 00 06 01 03 00 10 00 04
7315	2009-05-06 17:48:14.138	TCP	RCV	8741	0	1	17	22 25 00 00 00 0B 01 03 08 00 00 00 00 00 00 00
7316	2009-05-06 17:48:14.142	TCP	SND	8742	0	1	12	22 26 00 00 00 06 01 03 00 64 00 08
7317	2009-05-06 17:48:14.159	TCP	RCV	8742	0	1	9	22 26 00 00 00 03 01 83 02

Figure 157 Typical protocol analyzer output for Modbus TCP port.

Figure 158 shows a typical protocol analyzer output for the Modbus RS-485 port. It shows the following information for RS-485:

- **Seq.:** sequence number, which is automatically created in the device. This number is unique for one port.
- **Timestamp:** transmission time.

12 Operating Interfaces

12.1 Common Interface

12.1.1 Schedule and Calendar XML Files

The daily schedule and calendar pattern configuration can be changed at run-time over the Web UI or the network. An alternative way to change that configuration is to download a schedule and calendar XML file via FTP onto the device. After the file has been downloaded, the new configuration becomes effective immediately. The device does not need to be rebooted. The files are located in

```
/tmp/uid/sched/UID.xml  
/tmp/uid/cal/UID.xml
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 108. A schedule data point with UID 107C would result in the schedule XML file `/tmp/uid/sched/107C.xml`. The UID remains constant for the life time of the data point even when the name or description is changed.

The content of the XML file must be compliant to the scheduleCfg schema. This schema can be found at the LOYTEC Web site. The XML documents can refer to the target namespace <http://www.loytec.com/xsd/scheduleCfg/1.0/>

12.1.2 Trend Log CSV File

The CSV file format for a trend log and the location of those files are defined in this section. The trend log CSV files are accessible either via their UID only, or in combination with contents of the trend log object name. The files are located in

```
/tmp/uid/trend/UID.csv  
/data/trend/Datapointname_UID.csv
```

The *UID* is the unique ID of the data point. The UID can be obtained from the ID column in the data point list as shown in Figure 108. For a more user-friendly listing of the files, the *Datapointname* contains the trend log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the trend object 'trend0' and the UID '107C' would result in the CSV file `/data/trend/trend0_107C.csv`. The UID remains constant for the life time of the object even when the name is changed.

The CSV file format for a trend log is defined in this section. The CSV file starts with a header, containing at least the first line, which specifies the CSV format (log_csv_ver). The current version is 2. The next line contains the field log_device. It has trailing fields that specify the vendor, product code, firmware version and device ID string. The Device ID String can be one of the following: (IP) 192.168.24.100, (BACnet Device) 224100, (CEA-709 NID) NID.

The `log_info` line specifies the fields UID and name of the trend log object. The line `log_create` has two fields specifying the date and time when this CSV log was generated. The line `log_capacity` has two fields: the current number of log entries in the file and the log capacity.

Following are one or more lines of `log_item`. Each line specifies a trended data point. The first field is the index, the second the ID of the logged data point, the third the data point name. The data point name can be augmented by engineering units in square brackets. Log entries in the CSV refer to the item index to identify the data point, for which the entry was logged.

```
#log_csv_ver,2
#log_device;LOYTEC;Product Code;Firmware Version;Device ID String; Serial No
#log_info;Log-ID;Log Name
#log_create;YYY-MM-DD;HH:MM:SS
#log_capacity;filled;capacity
#log_item;index;UID;data point name [units]
```

After those lines any number of comment lines starting with a hash character '#' are allowed. One line contains the column headings. Lines that are not comments specify one log record per line, using the column information as described below. The columns are separated by commas ',' or semi-colons ';'. If commas are used as a separator, the decimal point must be a point '.'. If semi-colons are used, the decimal point must be a comma ','.

Column	Field	Example	Description
A	Sequence Number	50	The log record sequence number. This is the monotonously increasing sequence number, which is unique for each log record.
B	Source	0	Data point source identifier. Indexes into <code>logger_entry</code> header. For value lines in a multi-column CSV, this field indexes the first column, which has a value. For the ERROR record type, the field indexes the data source that caused the error. For LOGSTATE, TIMECHANGE records this field is not applicable and can be left at zero.
C	Record Type	2	The record type: LOGSTATE (0), BOOL (1), REAL (2), ENUM (3), UNSIGNED (4), SIGNED (5), NULL (7), ERROR (8), TIMECHANGE (9)
D	Error/Time Change/Log Status	1	This field is valid for records of type ERROR, TIMECHANGE, and LOGSTATUS.
E	Date/Time	2007-11-02 15:34:22	The date/time of the log record. This is in the format YYYY-MM-DD HH:MM:SS.
F	Value 0	24,5	Logged value from source 0 or empty
G	Value 1	200	Logged value from source 1 or empty
...	...		
...	Value $n - 1$	5000	Logged value from source $n - 1$ or empty

Table 9: Columns of the Trend Log CSV File.

There are as many value columns as value sources specified in the header. If at a given date/time more values are logged, all of them appear in the same line. If at that given time some sources did not log values, those columns are left empty. The "Source" column in a multi-value CSV refers to the first data source that supplied a value in a given line.

12.1.3 Alarm Log CSV File

The historical alarm logs are also accessible as CSV-formatted files. The alarm log CSV files are accessible either via their UID only, or in combination with contents of the alarm log object name. The files are located in

```
/tmp/uid/allog/UID.csv  
/data/allog/Alarmlogname_UID.csv
```

The *UID* is the unique ID of the alarm log object. The UID can be obtained from the ID column in the data point list of the alarm log folder, similar to obtaining the UID of trend log objects. For a more user-friendly listing of the files, the *Alarmlogname* contains the alarm log's object name. It is truncated after 23 ASCII characters to fit the requirements of the file system. A trend CSV file for the alarm log object 'alarmlog0' and the UID '100C' would result in the CSV file '/data/allog/alarmlog0_100C.csv'. The UID remains constant for the life time of the object even when the name is changed.

The CSV format of the alarm log CSV file is identical to the trend log CSV format as described in Section 12.1.2.

12.2 CEA-709 Interface

12.2.1 NV Import File

Network variables can be imported to the LINX-10X Configurator in a CSV file. The format of this file is described in this section.

The first line of the file must contain a comment, starting with a hash character '#' specifying the format version and import technology:

```
#dpal_csv_config;Version=1;Technology=CEA709
```

After that line any number of comment lines starting with the hash character '#' are allowed. Lines that are not comments specify one NV per line, using the column information as described in Table 10. The columns are separated by commas ',' or semi-colons ';'. Which separator is used can be configured in the Web UI (see Section 4.2.1).

Column	Field	Example	Description
A	SNVT	39	A numeric value of the SNVT (as defined in the SNVT master list). The example value 39 represents a SNVT_temp.
B	NV index	0	The NV index in decimal notation of the NV on the network node. Index starts at 0.
C	NV selector	1	The NV selector in decimal notation of the NV on the network node.
D	NV name	nvoTemp	The NV programmatic name of the NV on the network node.
E	is output	1	Defines if this NV is an output on the network node. '1' means the NV is an output on the network node.
F	flag auth cfg	1	'1' defines that authentication can be configured for this NV on the network node.
G	flag auth	0	'1' defines that the NV is authenticated.
H	flag priority cfg	1	'1' defines that the priority can be configured for this NV on the network node.
I	flag priority	0	'1' defines that the NV is using priority.
J	flag service type cfg	1	'1' defines that the service type can be configured for this NV on the network node.
K	flag service ack	1	'1' defines that the NV is using acknowledged service.
L	flag polled	0	'1' defines that the NV is using the polled attribute
M	flag sync	0	'1' defines that the NV is a synchronous NV.
N	Deviceref	1	This field is a numeric reference to a device description. If it is the first occurrence of this reference in the file, the columns defined below must be filled in. Otherwise, they can be left out.
O	programID	9000A44850060402	The program ID string of the network device.
P	neuronID	80000000C8C8	The NID of the network device.
Q	Subnet	2	The subnet address of the network device. Use '0' if the device has no subnet address information.
R	Node	3	The node address of the network device. Use '0' if the device has no node address information.
S	location str	0	The location string of the network device. Use '0' if no information is available.
T	Device name	DDC	The device name of the network device. Leave this field blank if this information is not available.
U	node self-doc	&3.2@0,2	Self-documentation string of the device (special characters are escaped)
V	NV length	2	NV length in bytes
W	NV self-doc	@0 4	NV self-documentation string (special characters are escaped)
X	Allocation	1	Define, how this NV shall be allocated: external=1 (default) / static=2 / file=3

Table 10: CSV Columns of the NV Import File.

12.2.2 Node Object

The LINX-10X provides a node object conforming to the LONMARK guidelines.

- The Node Object accepts the following commands via *nviRequest*: RQ_NORMAL, RQ_UPDATE_STATUS, RQ_REPORT_MASK, RQ_ENABLE, RQ_DISABLE, RQ_UPDATE_ALARM, RQ_CLEAR_ALARM, RQ_RESET, RQ_CLEAR_RESET

- LONMARK alarming is supported via *nvoAlarm* (SNVT_alarm) and *nvoAlarm_2* (SNVT_alarm_2). This allows devices supporting the LONMARK alarm notifier profile to receive alarms generated by the LINX-10X and react with a defined action (e.g., send an email). By supporting both alarm SNVTs, SNVT_alarm and SNVT_alarm_2, legacy and state-of-the-art alarm handling is supported.
- *nviDateEvent* (SNVT_date_event), *nvoDateResync* (SNVT_switch): These NVs are part of the standard LONMARK node object, if schedulers are used. If not bound, the local calendar is used. If a global calendar shall be used, both of these NVs must be bound to the respective NVs of the global calendar object.
- *nviTimeSet* (SNVT_time_stamp): When writing to this NV, the system is set. The time value is interpreted as local time
- *nvoSystemTemp* (SNVT_temp): This NV can be used to poll the system temperature of the LINX-10X. It does not send updates and must be polled.
- *nvoSupplyVolt* (SNVT_volt): This NV can be used to poll the supply voltage of the LINX-10X. It does not send updates and must be polled.
- *nvoIpAddress* (SNVT_str_asc): This NV can be used to poll the IP address of the LINX-10X. It does not send updates.
- *nciEarthPos* (SNVT_earth_pos): This configuration property can be used to set the earth position of the LINX-10X. It has been implemented as an NV to make other devices send that configuration to the LINX-10X over the network (e.g., from a GPS device).
- *nviClearStat* (SNVT_switch): When writing {100.0 1} to this NV, the channel monitor objects' statistics data are cleared.
- *nvoUpTime* (SNVT_elapsed_tm): This NV contains the elapsed time since the last reboot.

12.2.3 Real-Time Keeper Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the standard LONMARK real-time keeper object. The Real-Time Keeper Object is used to synchronize the system time of multiple LonMark compliant devices.

The object has the following network variables:

- *nvoTimeDate* (SNVT_time_stamp): Propagates the devices current system time and date (local time). It is typically bound to the *nviTimeSet* input network variable of the node objects of the LonMark compliant devices, which are synchronized with the system time of the LINX-10X. The update rate of the *nvoTimeDate* can be configured using the configuration property SCPTupdateRate (default every 60 seconds).

12.2.4 Channel Monitor Object

The Channel Monitor Object functional block is responsible for network monitoring. There is one object for each channel, the LINX-10X is attached to: The channel monitor object with index 0 corresponds to the FT port of the LINX-10X, while the object with index 1 corresponds to the IP-852 port of the LINX-10X. If a port is not available in the current system configuration, the *nvoElapsedTime* is set to the invalid value and *nvoPort* is set to 255.

Each object has the following network variables:

- *nvoPort* (SNVT_count): Index of port associated with this Channel Monitor Object instance. Port 1 corresponds to the FT port of the LINX-10X, while port 2 corresponds to the IP-852 port of the LINX-10X. If the monitored port is not available in a system configuration, the value is 255. This NV is polled only.

- *nvoElapsedTime (SNVT_elapsed_tm)*: Time since LINX-10X powered up or since the statistics for this port where reset. The statistics can be reset with the network variable *nviClearStat* in the node object (see Section 12.2.2) or if the node is reset with a network management command (e.g., while the device is commissioned). If the monitored port is not available in a system configuration, the value is set to the invalid value. The NV is polled only.
- *nvoAvgPkts (SNVT_count_32)*: The average number of packets per second received or transmitted via the associated channel since power-up or since the statistics for this port where reset.
- *nvoIvalBandUtl (SNVT_lev_cont)*: Bandwidth utilization of associated channel during the last interval. For a smooth operation of the CEA-709 segment, the average bandwidth utilization must remain below 50 %.
- *nvoIvalCrcErr (SNVT_lev_cont)*: Percentage of packets with CRC error received on the associated channel during the last interval.
- *nvoIvalMissed (SNVT_lev_cont)*: Percentage of packets from the associated channel which could not be processed during the last interval.
- *nvoIvalPkts (SNVT_count_32)*: Number of packets received or transmitted via the associated channel during the last interval.
- *nvoTotalCrcErr (SNVT_count_32)*: Total number of packets with CRC error received via the associated channel since power-up or since the statistics for this port where reset.
- *nvoTotalMissed (SNVT_count_32)*: Total number of packets from the associated channel which could not be processed since power-up or since the statistics for this port where reset.
- *nvoTotalPkts (SNVT_count_32)*: Total number of packets received or transmitted via the associated channel since power-up or since the statistics for this port where reset.
- *nvoMaxBandUtl (SNVT_lev_cont)*: Maximum value of *nvoIvalBandUtl* since power-up or since the statistics for this port where reset. For a smooth operation of the CEA-709 segment the average bandwidth utilization must remain below 50 %.
- *nvoMaxCrcErr (SNVT_lev_cont)*: Maximum value of *nvoIvalCrcErr* since power-up or since the statistics for this port where reset.
- *nvoMaxMissed (SNVT_lev_cont)*: Maximum value of *nvoIvalMissed* since power-up or since the statistics for this port where reset.
- *nvoMaxPkts (SNVT_count_32)*: Maximum value of *nvoIvalPkts* since power-up or since the statistics for this port where reset.
- *nvoIvalMisPre (SNVT_count_32)*: Number of missed preambles per second on the associated channel measured during the last interval. A missed preamble is detected whenever the link layer receives a preamble which is shorter then the defined preamble length. A large number in this counter is usually due to noise on the channel.
- *nvoTotalMisPre (SNVT_count_32)*: Total number of missed preambles per second on the associated channel measured since power-up or since the statistics for this port where reset.
- *nvoMaxMisPre (SNVT_count_32)*: Maximum value of *nvoIvalMisPre* since power-up or since the statistics for this port where reset.
- *nvoChnlAlarm (SNVT_switch)*: Signals an overload alarm condition of the channel during the last statistic interval. A channel can be overloaded due to one of the following conditions:
 - The bandwidth utilization during the last statistic interval (*nvoIvalBandUtl*) exceeded the limit defined by the *SCPThighLimit1* (default 70 %) OR

- o The CRC Error Rate during the last statistic interval (*nvoIvalCrcErr*) exceeded the limit defined by the *SCPThighLimit1* (default 5 %) OR
- o The Missed Packets Rate during the last statistic interval (*nvoIvalMissed*) was not zero OR
- o The Missed Preamble Rate during the last statistic interval (*nvoIvalMisPre*) exceeded the limit defined by the *SCPThighLimit1* (default switched off).

If an overload is detected, the network variable is set to {100, ON}. If no error occurred, it is set to {0, OFF}.

- *nvoChnlAlarmRat* (*SNVT_lev_cont*): Ratio between statistic intervals during which the channel was in overload alarm condition and intervals during which the channel was not in overload alarm condition since power-up or since the statistics for this port were reset.

In addition, each channel monitor object has the following SCPTs:

- *SCPTifaceDesc*: This configuration property contains a human-readable name of the monitored port. Possible values on the LINX-10X are “CEA-709”, “IP”, or “inactive”.
- *SCPTmaxSndT*: Defines how often output NVs are transmitted. Exceptions are *nvoPort*, and *nvoElapsedTime*, which are polled-only.

12.2.5 Calendar Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the standard LONMARK calendar object.

12.2.6 Scheduler Object

When the scheduler objects are enabled in the project settings, the LINX-10X includes the configured number of standard LONMARK scheduler objects.

12.2.7 Clients Object

When the remote AST object feature is enabled in the project settings, the LINX-10X includes a proprietary object, which is a container for network variables required to implement the remote object features.

For remote schedulers and calendars, *nviSchedLink* and *nviCalLink* NVs are created. For alarm clients, *nviAlarm_2* NVs are created.

12.2.8 Gateway Objects

The LINX-10X contains eight proprietary Gateway objects. These are containers for all NVs which are configured on the LINX-10X's CEA-709 port. They are intended for grouping NVs. When static NVs are created, they can be assigned to any of the eight gateway blocks. When creating dynamic NVs in the LNS-based tool, the NVs should be added to the gateway blocks.

13 Network Media

13.1 FT

The LINX-10X FT port is fully compatible to the parameters specified by LONMARK for this channel. FT ports can also be used on Link Power (LP-10) channels. However, the LINX-10X does not provide the power supply for Link Power channels.

When using the Free Topology Segment feature of the FT, only one termination (Figure 159) is required and can be placed anywhere on the free topology segment. Instead of building the termination, one can order the L-Term module (LT-33) from LOYTEC, which can be used to properly terminate the bus.

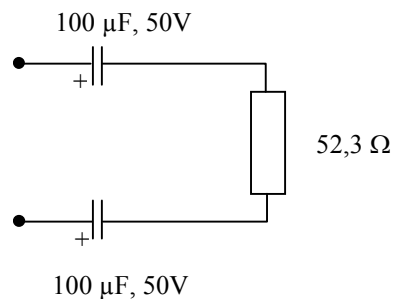


Figure 159: FT Free Topology Termination.

In a proper bus topology, two terminations are required (Figure 160). These terminations need to be placed at each end of the bus. Here, also L-Term modules can be used at either end.

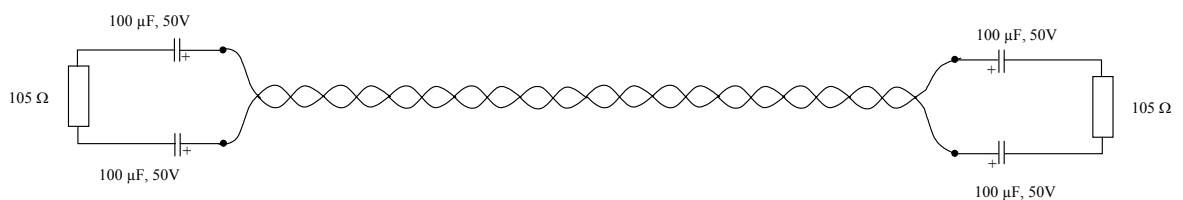


Figure 160: Termination in an FT Bus Topology.

13.2 M-Bus

The LINX uses the RS-232 console interface for the connection to an external M-Bus transceiver (repeater). The M-Bus specifies no special topology requirement, though it is not advised to use a ring topology. A maximum of 250 M-Bus slave devices can be connected to the bus, in fact, the external bus transceiver can have a lower limit of connected devices. Please refer to the datasheet of the transceiver used for more detailed information. The usual cabling is a standard telephone wire (JYStY N*2*0.8 mm). The maximum distance between a slave and the repeater is 350 meters at Baud rates from 300-9600 Baud; by limiting the Baud rates and using fewer slaves, this limit can be increased. Additionally, it must be ensured that the bus voltage does not fall below 12 V. The maximum cable length of the system must not exceed 1000 m (maximum cable capacitance of 180 nF).

13.3 Modbus RS-485

The LINX-10X Modbus RS-485 port is an electrical interface in accordance to EIA-485. The topology of the Modbus RS-485 consists of a trunk cable, along which the devices are connected either directly or via short derivation cables. Without repeater a maximum of 32 slave devices can be connected to the bus. Each Modbus RS-485 network segment must be properly terminated with an LT-04 network terminator connected at each of the two ends of the segment media. Some Modbus slave devices might require the use of external pull-up and pull-down resistors. Please refer to the data sheet or user manual of the slave device. Figure 161 shows the Modbus RS-485 network including pull-up and pull-down resistor and the network termination.

The maximum length of the cabling depends on the Baud rate used. Without repeater a maximum length of 1000 meters is possible at 9600 Baud. According to the Modbus standard the derivation cabling must never exceed 20 m.

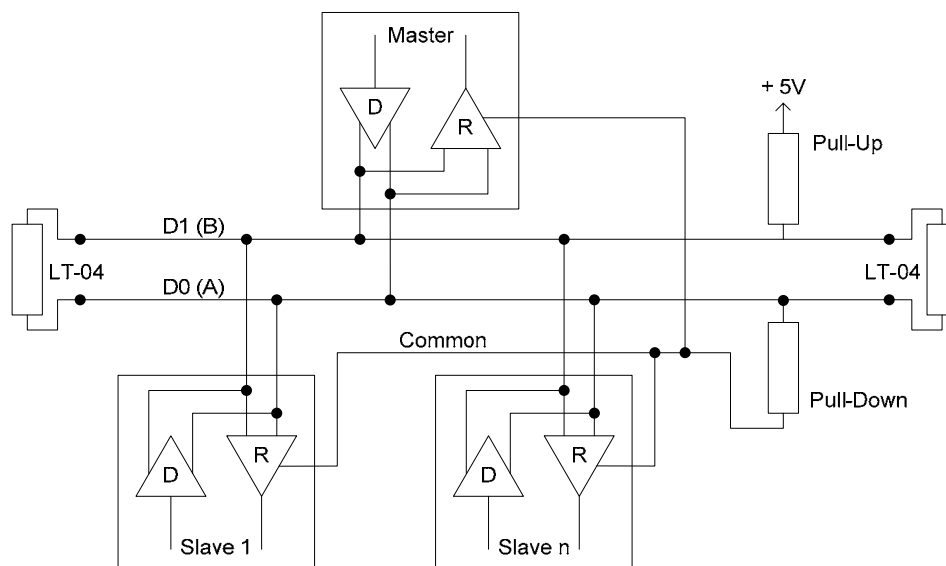


Figure 161: Modbus RS-485 network

14 LINX-10X Firmware Update

The LINX-10X firmware supports remote upgrade over the network and the serial console.

To guarantee that the LINX-10X is not destroyed due to a failed firmware update, the LINX-10X firmware consists of two images:

- LINX-10X fallback image,
- LINX-10X primary image.

The LINX-10X fallback image cannot be changed. Thus, if the update of the primary image fails or the image is destroyed by some other means, the fallback image is booted and allows reinstalling a valid primary image.

When the LINX-10X boots up with the fallback image, the OPC LED, the CEA-709 port LED and the CNIP LED are flashing red.

14.1 Firmware Update via the LINX-100/200 Configurator

The LINX-10X primary image can be updated using the LINX-100/200 Configurator. For this purpose, the LINX-10X must be connected to the Ethernet and must have a valid IP configuration (see Section 4.2.4). The LINX-100/200 Configurator must be installed (see Section 6.1).

To Update the Firmware using the LINX-100/200 Configurator

1. Start the LINX-10X Configurator from the Windows Start menu: **Start → Programs → LOYTEC LINX-100 Configurator → Configure LINX-100**.
2. Select the menu: **Connection → Connect via FTP**. This opens the FTP connection dialog as shown in Figure 162.

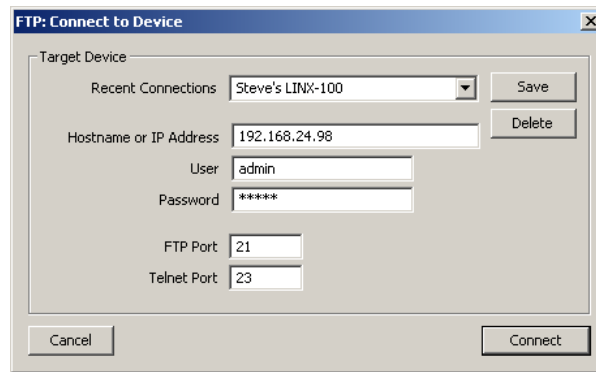


Figure 162: FTP connection dialog.

3. In the FTP connection dialog, enter the IP address of the LINX-10X as well as the FTP user name and password. The default user name and password are 'admin' and 'admin'. This can be changed via the Web interface (see Section 4.1) and reset via the console UI (see Section 15.2.2).
4. Click on **Connect**.
5. Select the menu: **Firmware → Update ...**
6. This opens the Firmware Update dialog as shown in Figure 163. Click on the button "..."

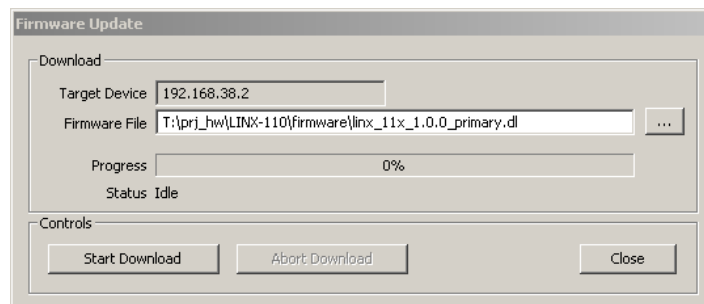


Figure 163: Firmware Update dialog of the LINX-100/200 Configurator.

7. Click on **Start Download**.
8. Observe the download progress. When the download is complete, the dialog shown in Figure 164 appears.

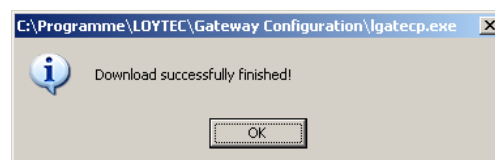


Figure 164: FTP download success dialog.

9. Click **OK**.
10. In the Firmware Update dialog, click **Close**.
11. The device's firmware has now been successfully upgraded.

14.2 Firmware Update via the Console

To download the firmware via the console interface, the LINX-10X must be connected to the RS-232 port of a PC via its console interface as described in Section 15.2.1. You will need the LOYTEC serial upgrade tool (LSU Tool), which can be downloaded from our homepage at www.loytec.com.

Please make sure that the LINX-10X console shows the main menu. Otherwise navigate to the main menu or simply reset the LINX-10X.

To Upgrade via the Console

1. Double click on the *.dlc file that comes with the new firmware package. This should start the LSU Tool and load the firmware image referenced in the dlc file. Please note that the dlc file and the dl file must be stored in the same folder. The start window of the LSU tool is shown in Figure 165.

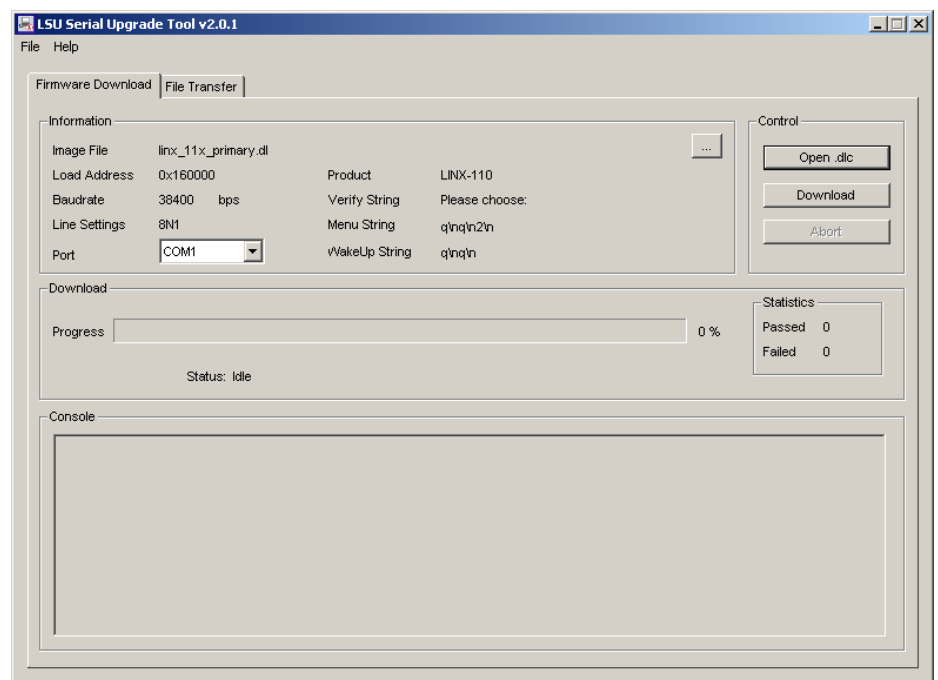


Figure 165: LSU Serial Upgrade Tool in Idle Mode.

2. If the LINX-10X is not connected to COM1 you can change the port to COM2, COM3, or COM4. Make sure that the product shown under "Product" matches the device you are upgrading. Press **Download** to start the download. A progress bar as shown in Figure 166 can be seen.

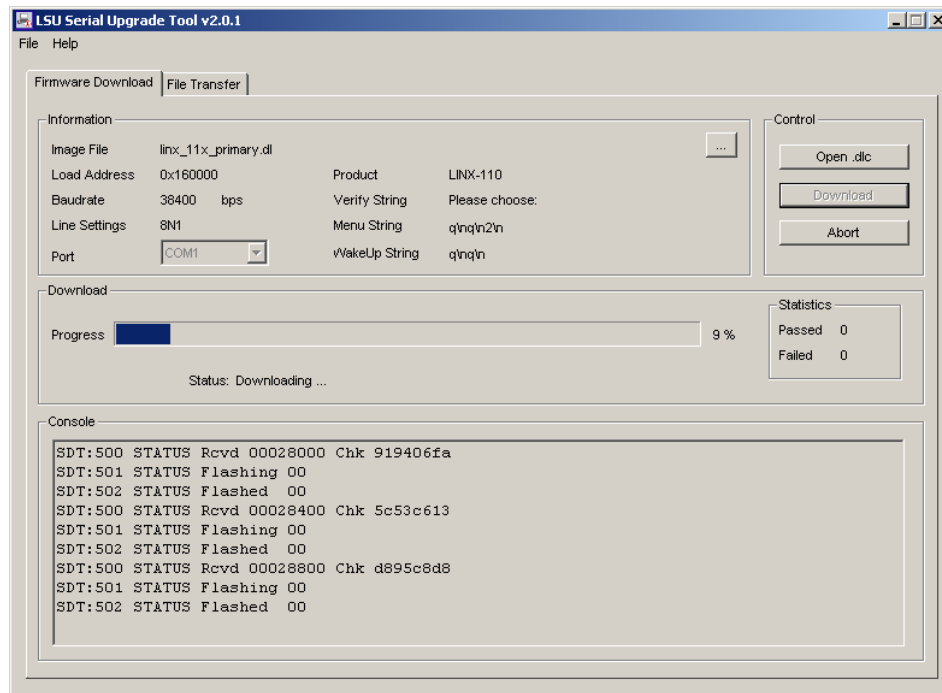


Figure 166: Progress Bar during Firmware Download.

3. If the upgrade is successful, the following window appears (Figure 167).

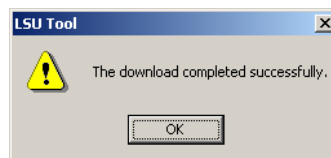


Figure 167: Successful Firmware Upgrade.

4. Double check that the new firmware is executed by selecting '1' and pressing **Enter** in the console window. This will bring up the device information which shows the current firmware version.

15 Troubleshooting

15.1 Technical Support

LOYTEC offers free telephone and e-mail support for the LINX-10X product series. If none of the above descriptions solves your specific problem please contact us at the following address:

*LOYTEC electronics GmbH
Blumengasse 35
A-1170 Vienna
Austria / Europe*

*e-mail : support@loytec.com
Web : http://www.loytec.com
tel : +43/1/4020805-100
fax : +43/1/4020805-99*

or

*LOYTEC Americas Inc.
11258 Goodnight Lane
Suite 101
Dallas, Texas 75229
USA*

*e-mail: support@loytec-americas.com
Web: http://www.loytec-americas.com
tel: +1/512/402 5319
fax: +1/972/243 6886*

15.2 Statistics on the Console

15.2.1 Connecting to the Console

Use a PC terminal program with the communication settings set to 38,400 bps / 8 data bits / no parity / 1 stop bit / no handshake. To connect COM1 of the PC to the Console on the device, use a standard null-modem cable with full handshaking. Power up the device or press **Return** if the device is already running. The menu shown in Figure 168 should appear on the terminal.

```
Device Main Menu
=====

[1] Show device information
[2] Serial firmware upgrade
[3] System configuration
[4] CEA-709 configuration
[5] IP configuration
[6] CEA-852 device configuration
[7] CEA-852 server configuration
[8] Reset configuration (factory defaults)
[9] Device statistics
[c] Modbus configuration

[a] Data Points

[0] Reset device

Please choose:
```

Figure 168: Console Main Menu.

15.2.2 Reset configuration (load factory defaults)

Select item '8' in the console main menu. This menu item allows resetting the device into its factory default state. The menu appears as shown in Figure 169.

```
Reset Configuration Menu
=====

[1] Reset everything to factory defaults
[3] Reset all passwords
[4] Clear data point configuration

[q] Quit

Please choose:
```

Figure 169: Reset to Factory Defaults Menu.

Select option '1' to reset the entire device to factory defaults (including error log, configuration files, passwords etc.). Select option '3' to reset all passwords (Web interface, FTP server etc.) to factory defaults.

Select option '4' to clear all configured data points, such as CEA-709 network variables or user registers. This effectively clears the entire port configuration. The LINX-10X must be rebooted to let the changes take effect.

Note: This option does not reset the configuration of the built-in router of the LINX-101. The nodes connected by the router are still reachable after clearing the data point configuration.

15.2.3 Device Statistics Menu

Select '9' from the device main menu to get to the device statistics menu. This menu holds relevant information regarding the device statistics of the device. This section describes those statistics, which are not available on the Web UI. The device statistics menu is shown in Figure 170. Use this menu only for debugging purposes. There is no need to access this menu if the network is running smoothly.

```
Statistics Menu
=====

[4] Show IP statistics
[8] Show DPAL statistics
[9] Show Reg DPAL statistics

[q] Quit

Please choose:
```

Figure 170: Device Statistics Menu on the Console.

15.2.3.1 IP statistics

A sample console output is shown in Figure 171.

```
***** INTERFACE STATISTICS *****
***** lo0 *****
Address:127.0.0.1
Flags: Up Loopback Running Multicast
Send queue limit:50 length:0 Dropped:0
***** eth0 *****
Address:192.168.0.2 Broadcast Address:192.168.0.255
Flags: Up Broadcast Running Simplex Multicast
Send queue limit:50 length:0 Dropped:0
Network Driver Stats for CS8900 :
    rx ready len - 50 rx loaded len - 0
    rx packets - 931 tx packets - 165
    rx bytes - 78480 tx bytes - 13627
    rx interrupts - 931 tx interrupts - 165
    rx dropped - 0 rx no mbuf - 0
    rx no custers - 0 rx oversize errors - 0
    rx crc errors - 0 rx runt errors - 0
    rx missed errors - 0 tx ok - 165
    tx collisions - 0 tx bid errors - 0
    tx wait for rdy4tx - 0 tx rdy4tx - 0
    tx underrun errors - 0 tx dropped - 2
    tx resends - 0 int swint req - 2094
    int swint res - 2094 int lockup - 0
    interrupts - 3189

***** MBUF STATISTICS *****
mbufs: 512 clusters: 64 free: 14
drops: 0 waits: 0 drains: 0
    free:461 data:51 header:0 socket:0
    pcb:0 rtable:0 htable:0 atable:0
    soname:0 soopts:0 ftable:0 rights:0
    ifaddr:0 control:0 oobdata:0

***** IP Statistics *****
    total packets received 922
    datagrams delivered to upper level 922
    total ip packets generated here 158

Destination Gateway/Mask/Hw Flags Refs Use Expire
Interface
default 192.168.0.1 UGS 6 0 0 eth0
62.178.55.77 192.168.0.1 UGH 0 1 3606 eth0
62.178.95.96 192.168.0.1 UGH 0 1 3606 eth0
81.109.145.243 192.168.0.1 UGH 0 1 3606 eth0
81.109.251.36 192.168.0.1 UGH 0 1 3606 eth0
127.0.0.1 127.0.0.1 UH 0 0 0 lo0
130.140.10.21 192.168.0.1 UGH 1 6 0 eth0
192.168.0.0 255.255.255.0 U 0 0 3 eth0
192.168.0.1 00:04:5A:26:96:1F UHL 7 0 1722 eth0
213.18.80.166 192.168.0.1 UGH 1 148 0 eth0
***** TCP Statistics *****

***** UDP Statistics *****
    total input packets 924
    total output packets 158

***** ICMP Statistics *****
```

Figure 171: IP Statistics.

The IP statistics menu has the additional feature of displaying any IP address conflicts. If the device's IP address conflicts with another host on the network, the banner shown in Figure 172 is displayed.

```
WARNING: Conflicting IP address detected!
IP address 10.125.123.95 also used by device with MAC address
00 04 5A CC 10 41!
```

Clear IP conflict history (y/n):

Figure 172: IP Address Conflict.

As useful information, the MAC address of the conflicting host is shown. If the information about this conflict shall be cleared, enter 'y'. If 'n' is selected, the conflict will show up again the next time this menu is entered.

16 Application Notes

16.1 The LSD Tool

Please refer to application note “AN002E LSD Tool” for further information about the LOYTEC system diagnostics tool for the LINX-10X.

16.2 Use of Static, Dynamic, and External NVs on a Device

Please refer to application note “AN009E Changing Device Interface in LNS” for more information on the static NV interface, XIF files, device templates and the use of static, dynamic, and external NVs on LOYTEC gateway products.

17 Firmware Versions

Table 11 shows the most important features available only in certain firmware versions.

Firmware Version/ Features	3.0.0	3.1.0	3.2.0	3.3.0	3.4.0	3.5.0
OPC XML-DA Server	√	√	√	√	√	√
CEA-709 Network Scan	√	√	√	√	√	√
UNVTs, SCPTs	√	√	√	√	√	√
XML configuration	√	√	√	√	√	√
Connections	—	—	√	√	√	√
Scheduler	√	√	√	√	√	√
Trend Log	√	√	√	√	√	√
Min/max/average trends	—	√	√	√	√	√
Alarming	√	√	√	√	√	√
Alarm Log	√	√	√	√	√	√
E-mail	√	√	√	√	√	√
Backup/Restore Configuration	√	√	√	√	√	√
DL Web-Service 1.1	—	√	√	√	√	√
M-Bus	—	—	√	√	√	√
Modbus	—	—	—	√	√	√
Modbus Slave	—	—	—	—	—	√
Support for the Master Scheduler Configurator	—	—	—	—	√	√
Next state (SNVT_tod_event)	—	—	—	—	√	√
Embedded calendar	—	—	—	—	√	√
Run-Time Configuration	—	—	—	—	—	√

Table 11: Available Features depending on Firmware Version.

18 Specifications

18.1 LINX-10X

18.1.1 Physical Specifications

Operating Voltage	12 – 35 VDC or 12 – 24 VAC $\pm 10\%$
Power Consumption	typ. 3 W
In rush current	up to 950 mA @ 24 VAC
Operating Temperature (ambient)	0°C to +50°C
Storage Temperature	-10°C to +85°C
Humidity (non condensing) operating	10 to 90 % RH @ 50°C
Humidity (non condensing) storage	10 to 90 % RH @ 50°C
Enclosure	Installation enclosure 6 TE, DIN 43 880
Environmental Protection	IP 40 (enclosure); IP 20 (screw terminals)
Installation	DIN rail mounting (EN 50 022) or wall mounting

18.1.2 Resource Limits

Total number of data points	10000
OPC tags	2000
User registers	1000
NVs (static, dynamic)	1000
External NVs	1000
Alias NVs	1000 (both ECS and legacy mode)
Address table entries	512 (15 in legacy mode)
LONMARK Calendar objects	1 (25 calendar patterns)

LONMARK Scheduler objects	100 (max. AST configuration size 384KB, 64 data points per scheduler)
LONMARK Alarm Servers	1
Trend Logs	100 (total of 256 trended data points, total aggregated size 6 MB)
E-mail templates	100
Math objects	100
Alarm logs	10
M-Bus	1000
Modbus	2000
Connections	1000

19 References

- [1] L-IP User Manual, LOYTEC electronics GmbH, Document № 88065909, June 2006.
- [2] NIC User Manual, LOYTEC electronics GmbH, Document № 88067212, September 2008.
- [3] LWEB-800 User Manual, LOYTEC electronics GmbH, Document № 88074203, April 2009
- [4] LWEB-801 User Manual, LOYTEC electronics GmbH, Document № 88074703, April 2009.
- [5] L-VIS User Manual, LOYTEC electronics GmbH, Document № 88068512, August 2008.

20 Revision History

Date	Version	Author	Description
2007-02-08	1.0	STS	Initial revision V1.0 for L-OPC 1.0
2008-08-01	3.0	STS	Initial revision V3.0 for LINX-10X 3.0
2008-11-14	3.1	STS	Updated for LINX-10X firmware release 3.1
2009-02-13	3.2	PP	Added Section 6.3 Connections, Chapter 10 M-Bus
2009-05-14	3.3	PP	Updated for LINX-10X firmware release 3.3, added Chapter 11 Modbus, added section 6.2.5. Behavior on Value Changes, added section 6.2.6 Custom Scaling, added section 7.8.2. Create Connections from a CSV File
2009-06-29	3.4	STS	Updated for LINX-10X firmware release 3.4. Section 6.4.3 withdraw, invalid, temp disable, embedded calendar, next-state feature, Section 7.2.3 renumber, filter, include subfolders, added Section 7.8 Advanced CEA-709 configuration, including installing unconfigured devices, Section 7.11.7 configure embedded exceptions, Section 7.11.8 configure scheduler control data points, Section 7.11.9 using SNVT_tod_event, updated Section 7.11.11 for scheduling parts of structured NVs, Section 7.15 added COV delta to math objects, replace data points. Added Section 14.2 M-Bus cabling, added Section 14.3 Modbus cabling.
2010-02-26	3.5	STS	Updated for LINX-10X firmware release 3.5. Removed Section on Console UI and added console statistics as Section 15.2. Added Section 4.2.3 port configuration Web UI. Added Section 4.2.12 trend configuration Web UI. Added Section 4.2.14 scheduler re-configuration Web UI. Added Section 6.2.5: Managing Multistate Maps. Section 6.3 Project settings: UNVT cut-out, added ASTv2 to project settings, updated download defaults, added device configuration tab. Section 6.7.6 Scanning NVs online from the Network: Updated to new CEA-709 management dialog. Section 6.7.9 Create Static NVs: updated new create dialog. Section 6.8.1 Importing devices from XIF templates. Section 6.8.2 Reset button in install dialog. Added Section 6.8.3: Using Feedback Data Points. Section 6.12.2 Create an Alarm Condition: Added enable, limit data points. Section 6.12.4 Added alarm log fill level notification. Section 9.2: New L-WEB project manager. Section 10.5.1 M-Bus secondary address scanning, new activation in project settings. Section 11.3.1 Modbus speeds 1200, 2400, 4800. Section 11.4.1 Modbus slave, device config in project settings. Section 18.1.2 Resource Limits: 2000 OPC tags.